



## **Anexo IX**

### **Termo de Referência do Sistema Integrado de Bilhetagem Eletrônica e Monitoramento (SIBEM)**

## ÍNDICE

1.	Descrição da Arquitetura .....	5
1.1.	Introdução .....	5
1.1.1.	Situação Atual .....	5
1.1.2.	Objetivo .....	5
1.1.3.	Premissas .....	5
1.2.	Visão Geral .....	7
1.3.	Sistema Integrado de Bilhetagem Eletrônica e Monitoramento .....	8
1.3.1.	Emissão de Cartões .....	8
1.3.2.	Sistema de Cadastramento de Usuários .....	8
1.3.3.	Utilização - Viagens .....	9
1.3.4.	Sistema Atendimento ao Usuário .....	9
1.3.5.	Vendas e Carga/ Recarga de Créditos Eletrônicos .....	9
1.3.6.	Monitoramento .....	10
1.3.7.	Comunicação com Usuário .....	10
1.3.8.	CCI - CENTRO DE CONTROLE DE INFORMAÇÃO (Data Center ARTESP) ..	10
1.3.9.	Segurança .....	10
1.4.	CCO - Centro de Controle Operacional – Concessionárias .....	11
1.4.1.	Rede de Comunicação de Dados .....	11
1.4.2.	CCO - Centro de Controle Operacional .....	13
1.4.3.	Central de Atendimento .....	14
1.4.4.	Integração entre ARTESP e Operadores .....	15
1.5.	Auditoria .....	15
1.6.	Contingência .....	16
2.	Sistema de Bilhetagem e Monitoramento .....	20
2.1.	Processos Suportados .....	20
3.	Transações / Processos Sistêmicos .....	22
3.1.1.	Processos Comuns ao Rodoviário e Suburbano .....	22
3.1.2.	Processos da Modalidade Suburbana .....	28
3.1.3.	Processos da Modalidade Rodoviária .....	39

3.2. Cadastramento e Manutenção de Parâmetros do Sistema. ....	43
3.3. Monitoramento - Envio de Informações para o CCO .....	44
3.4. Segurança .....	45
3.4.1. Geração, Armazenamento e Transporte de Chaves Primárias .....	45
3.4.2. Certificação de Créditos .....	45
3.4.3. Fiscalização de Transações de Viagem .....	46
3.4.4. Fiscalização de Transações de Créditos.....	47
3.4.5. Certificação de Arquivos .....	47
3.4.6. Geração e armazenamento de crédito .....	47
3.4.7. Transferência de Crédito do HSM para o SAM de PDV .....	48
3.4.8. Transferência de Crédito do SAM para Cartões de Usuário .....	49
3.5. Níveis de Serviço .....	50
4. Migração da Situação Atual para o Modelo ARTESP .....	50
5. Itens de Segurança .....	51
5.1. HSM - Hardware Security Module .....	51
5.2. Geração, armazenamento e transporte de chaves primárias .....	54
5.2.1. SAM .....	54
5.2.2. Máquina de Estados.....	55
5.2.3. Requisitos dos Cartões .....	56
6. Eletrônica Embarcada .....	57
6.1. Itens Comuns ao Suburbano e Rodoviário .....	57
6.1.1. Validadores .....	57
6.1.2. Terminal de Dados .....	60
6.1.3. Dispositivo de Geoposicionamento e Comunicação - DGC .....	61
6.2. Itens Exclusivos Suburbano.....	63
6.2.1. Validador na Saída do Ônibus .....	63
6.2.2. Catraca Eletrônica.....	64
6.3. Item exclusivo do Rodoviário .....	65
6.3.1. Contador de Passageiros.....	65
7. Cartões Inteligentes e Equipamentos de Venda.....	67
7.1. Cartões Inteligentes .....	67
7.1.2. Utilização do Cartão Eletrônico .....	68

7.2. Terminal de Venda .....	70
7.3. Equipamento de Autoatendimento.....	72
8. Equipamentos de Informação ao Usuário .....	74
8.1. Displays do Sistema de Informação .....	74
9. Fornecedores de Itens Pertinentes ao Sistema .....	75
9.1. Homologação de Fornecedores e Dispositivos.....	75

## 1. Descrição da Arquitetura

### 1.1. Introdução

#### 1.1.1. Situação Atual

A ARTESP - Agência Reguladora de Serviços Públicos Delegados de Transporte do Estado de São Paulo é um órgão vinculado à Secretaria Estadual de Governo do Estado de São Paulo, sendo de sua atribuição efetuar a regulação dos serviços rodoviários intermunicipais de transporte coletivo de passageiros no Estado de São Paulo no âmbito de sua competência.

O sistema de transporte rodoviário intermunicipal de passageiros é executado por meio de permissões, às empresas privadas, a operarem linhas, e são remuneradas em função da emissão de bilhetes, através da tarifa fixada em função da distância de linhas e seccionamentos tarifários (coeficiente quilométrico).

O presente documento é parte do processo licitatório de concessão de áreas de operação dos serviços rodoviários intermunicipais de transporte coletivo de passageiros para Operadores privados.

#### 1.1.2. Objetivo

Este Termo de Referência tem como objetivo estabelecer o escopo básico dos processos de bilhetagem e monitoramento, bem como os requisitos funcionais e técnicos estabelecidos pela ARTESP, a serem atendidos pelo SIBEM - Sistema Integrado de Bilhetagem Eletrônica e Monitoramento das Concessionárias, integrados ao Centro de Controle de Informação (CCI) da ARTESP.

#### 1.1.3. Premissas

As CONCESSIONÁRIAS deverão fornecer todas as informações do SIBEM para a ARTESP.

As Concessionárias deverão fornecer, para cada área de concessão, *logins* e senhas do SIBEM para a ARTESP. Estes usuários poderão fazer consultas e *downloads*, com diferentes níveis de autorização.

A ARTESP terá acesso, de visualização e *download*, a todas as informações contidas no SIBEM.

Todos os dados do SIBEM serão armazenados pela Concessionária pelo período do contrato. Deverão ficar disponíveis para consultas *online* os dados dos últimos 12 meses. Para dados com mais de 12 meses, a Concessionária deverá fornecer as informações solicitadas pela ARTESP em até 48 h.

As Concessionárias adquirirão equipamentos (hardware) e softwares que deverão atender a requisitos estabelecidos pela ARTESP para compor o SIBEM e a integração ao CCI. Os requisitos técnicos serão definidos em portaria específica.

As empresas fornecedoras de equipamentos (hardware) e softwares a serem adquiridos pelas Concessionárias deverão ser homologadas pela ARTESP, de acordo com portaria específica a ser publicada. Esta homologação consiste em verificar e validar a “qualificação técnica” da empresa e dos produtos no atendimento dos requisitos funcionais e técnicos do próprio SIBEM, bem como a integração com o CCI.

Somente as empresas fornecedoras homologadas poderão ser contratadas pelas Concessionárias do Sistema como fornecedoras de equipamentos e softwares a serem integrados ao CCI da ARTESP.

As Concessionárias poderão utilizar equipamentos e softwares adicionais, embarcados ou não, de forma a suportar suas aplicações proprietárias, desde que estes não interfiram na operação dos equipamentos básicos definidos neste instrumento e necessários para a integração ao CCI da ARTESP.

O CCI – Centro de Controle de Informação é um sistema de uso interno da ARTESP.

A solução de Bilhetagem Eletrônica deverá permitir a utilização de Cartão Inteligente de protocolo aberto, que seja interoperável com todas as Concessionárias para ambas as modalidades: rodoviária e suburbana.

O *mapping* dos Cartões Inteligentes, que consiste no mapa da sua estrutura lógica e de dados, deverá ser único para todo o SIBEM - Sistema Integrado de Bilhetagem Eletrônica e Monitoramento das Concessionárias, conforme portaria ARTESP a ser publicada.

Os módulos (Chip) SAM – Modulo de Segurança de Acesso (Secure Access Module), homologados pela ARTESP, deverão ser adquiridos pelas Concessionárias e entregues à ARTESP para gravação do software de segurança, estando aptos para instalação nos equipamentos.

Os fabricantes de SAM devem ser homologados junto a ARTESP atendendo critérios específicos de segurança, a serem definidos pela ARTESP em portaria.

Cada chip produzido deve ter a garantia de procedência e identificador único, determinando inclusive o fabricante.

Os chips SAMs serão especializados sendo no mínimo os seguintes:

- SAM para inicialização do chip
- SAM para operação de crédito
- SAM para operação de débito
- SAM com operação de crédito e débito

A ARTESP irá personalizar os SAMs após a aquisição por parte das concessionárias.

Todo SAM que entrar no sistema terá seu identificador único registrado no sistema da ARTESP. Sendo assim, se um crédito ou passagem for gerado por um SAM não registrado, o mesmo não será aceito e o cartão, bloqueado.

O chip a ser incorporado no cartão inteligente terá seu fornecedor e produto homologado junto a ARTESP. Este procedimento irá garantir os padrões de qualidade, segurança e, principalmente, o protocolo aberto definido pela ARTESP. Todo chip produzido deve ter um identificador único que permita o rastreamento do fabricante e do próprio chip.

A fabricação do cartão e sua personalização elétrica demandam o acesso *online* a ARTESP para receber via o HSM-SAM a chave de ativação do cartão e/ou a de personalização elétrica que irá gravar a(s) aplicação(ões). Cada etapa terá uma chave diferenciada.

## 1.2. Visão Geral

Os tópicos abaixo descrevem o escopo dos processos realizados pelas Concessionárias que deverão possuir interface com SIBEM - Sistema Integrado de Bilhetagem Eletrônica e

Monitoramento. Estes processos terão suporte nos componentes de hardware e software, apresentados neste Termo de Referência.

Somente os requisitos técnicos e funcionais sob responsabilidade das empresas Concessionárias serão definidos neste Termo de Referência.

O detalhamento das interfaces entre o SIBEM de responsabilidade das Concessionárias e o CCI da ARTESP será fornecido ao vencedor do processo licitatório de cada área de operação.

### **1.3. Sistema Integrado de Bilhetagem Eletrônica e Monitoramento**

#### **1.3.1. Emissão de Cartões**

Consiste na inicialização lógica dos Cartões Inteligentes, de acordo com as características dos diversos tipos de usuários e produtos para os quais o sistema será desenvolvido.

Os cartões deverão também ser personalizados de acordo com as características dos diversos tipos de usuários e produtos existentes no sistema.

#### **1.3.2. Sistema de Cadastramento de Usuários**

Consiste na identificação do usuário junto à Concessionária, onde serão caracterizados o tipo de usuário e a forma de utilização do cartão, qualificando-o dentro do sistema, bem como permitindo a personalização externa e/ou interna do sistema.

Compreende:

- I. Controle do Fornecimento de Cartões Inteligentes especiais para beneficiários de isenções totais e parciais de tarifação no acesso ao transporte suburbano, de acordo com a legislação vigente.
- II. Controle e registro da associação de Cartão Inteligente ao respectivo usuário.
- III. Controle da distribuição de Cartões Inteligentes aos usuários e às unidades de comercialização.



### 1.3.3. Utilização - Viagens

As transações de viagens (débito da tarifa nos Cartões Inteligentes) realizadas pelos usuários nos veículos deverão ser armazenadas na memória não volátil do validador e assinadas pelo SAM instalado no próprio validador, utilizando chaves e algoritmos que fazem parte do sistema de segurança do SIBEM.

### 1.3.4. Sistema Atendimento ao Usuário

O Sistema de Atendimento ao Usuário deverá realizar o registro de consultas, denúncias reclamações e/ou sugestões por parte dos usuários. Deverá ser utilizado também para registro de perdas, roubos ou danificação do Cartão Inteligente pelos respectivos usuários. Este subsistema é de responsabilidade da Concessionária. Pelo *login* e senha do SIBEM fornecido à ARTESP, esta poderá consultar e fazer *download* de toda e qualquer informação do SAU.

### 1.3.5. Vendas e Carga/ Recarga de Créditos Eletrônicos

Existem os seguintes tipos de Vendas de Créditos eletrônicos:

- I. Compra e pagamento de um lote de créditos eletrônicos realizados por adquirentes (credenciadas ou empresas - VT - Vale Transporte, VE - Vale Escolar) e liberação para recarga *online* por lista para seus beneficiários.
- II. Compra, pagamento e carga *online* por um usuário habitual de unidades de comercialização de créditos eletrônicos: bilheterias, pontos de vendas de terceiros e máquinas de autoatendimento.
- III. Compra, pagamento e utilização de viagem unitária em modalidade suburbana por um usuário eventual em bilheterias, terminais e veículos.
- IV. Para a modalidade rodoviária as passagens emitidas em papel poderão ser pagas com o Cartão Inteligente nas bilheterias e pontos de venda.

As transações de vendas de créditos eletrônicos e vendas de passagens em papel deverão ser armazenadas na memória não volátil dos terminais de venda ou equipamentos de autoatendimento, assinadas pelo SAM instalado nesses equipamentos, utilizando chaves e algoritmos que fazem parte do sistema de segurança.

### 1.3.6. Monitoramento

Através do dispositivo de geoposicionamento e comunicação (DGC) embarcado no ônibus será realizado o envio de eventos (mensagens) programados e/ou pré-definidos de forma *online* ao SIBEM:

- I. O embarque e o desembarque dos passageiros deverão ser registrados e acumulados nos veículos sendo descarregados nos pontos de coleta e transmitidos ao SIBEM e ao CCI da ARTESP. Estes eventos serão assinados utilizando módulo SAM no equipamento embarcado.
- II. Posicionamento e informações sobre o veículo (coordenadas GPS), em intervalos de tempo que serão definidos adiante. Estes eventos serão assinados utilizando módulo SAM presente no DGC.

### 1.3.7. Comunicação com Usuário

Este sistema estará disponível nos terminais de embarque e desembarque de passageiros e refere-se à comunicação com o usuário, disponibilizando informações de partidas e chegadas de veículos nestes terminais e consultas de horários, itinerários, preços de passagens, etc.

Para isso serão utilizados equipamentos descritos no item 8.

Este sistema é de responsabilidade da Concessionária.

### 1.3.8. CCI - CENTRO DE CONTROLE DE INFORMAÇÃO (Data Center ARTESP)

O CCI – CENTRO DE CONTROLE DE INFORMAÇÃO, instalado no Data Center da ARTESP, será responsável pela busca de informações operacionais nas bases de dados do sistema SIBEM de cada concessionária, disponibilizadas para a ARTESP. Este sistema é de responsabilidade da ARTESP.

### 1.3.9. Segurança

O Sistema de Segurança é responsável pela geração e verificação da assinatura digital que garante a segurança dos créditos eletrônicos, das informações (transações) e dos cartões do sistema. Este sistema é de responsabilidade das Concessionárias.

#### 1.4. CCO - Centro de Controle Operacional – Concessionárias

A Concessionária deverá implantar o CCO – CENTRO DE CONTROLE OPERACIONAL, com no mínimo as seguintes componentes:

- Registro das Ocorrências Operacionais;
- Central de Atendimento e Comunicação com o Usuário;
- Monitoramento das Viagens.

O CCO deverá apresentar numa única tela o mapa do Estado de São Paulo com a viagem (origem e destino) dentro da área de concessão, a identificação do veículo, placa, nome e foto do motorista, horários programados de partida e chegada, horários efetivos de partida e chegada, status da documentação, dados de GPS (deslocamento, velocidade atual e média horária) e geoposicionamento do veículo. Deverá, ainda, mostrar a identificação da viagem, lista de passageiros com nomes e documento de identificação, lista de gratuidade, lista de idosos e lista de estudantes.

O CCO deve operar 24 horas ininterruptamente com sua base de dados e disponibilizar em tempo real os dados para o CCI da ARTESP.

##### 1.4.1. Rede de Comunicação de Dados

A concessionária deverá dimensionar, implantar, operar e manter todas as redes de comunicações, físicas ou não, de transferência de dados, comandos e informações entre todos os componentes do SIBEM, sendo no mínimo:

- I. Entre os equipamentos instalados nas unidades de comercialização, nas unidades de atendimento ao usuário e o CCO.

Estas redes de comunicação deverão ter características de confiabilidade e disponibilidade que possibilitem, pelo menos a realização *online* das seguintes operações:

- i. Transmissão de todas as transações de venda de créditos pendentes de envio por parte dos equipamentos;

ii. Recebimento das novas versões de parâmetros e software para atualização por parte dos equipamentos;

iii. Abastecimento de créditos para distribuição *offline* nos equipamentos.

II. Entre os equipamentos instalados nos veículos e o CCO.

Estas redes de comunicação deverão ter características de confiabilidade e disponibilidade que possibilitem a realização *online* das seguintes operações:

i. Transmissão de todas as transações de utilização de créditos e monitoramento de frota, pendentes de envio, por parte dos equipamentos;

ii. Recebimento das novas versões de parâmetros e software para atualização por parte dos equipamentos.

III. Entre o CCO e os equipamentos de informação ao usuário.

Estas redes de comunicação deverão ter características de confiabilidade e disponibilidade que possibilitem o acesso *online* ao CCO por parte dos equipamentos, para obtenção de informações operacionais para atualização das informações aos usuários.

IV. Entre o CCO da concessionária e CCI da ARTESP.

As CONCESSIONÁRIAS deverão enviar todos os dados ao CCI da ARTESP. O envio de dados deverá ser *online* e ter características de confiabilidade e disponibilidade. Com especial atenção para:

i. Transmissão de todas as transações de venda de créditos, utilização de créditos e monitoramento de frota, pendentes de envio, procedentes dos equipamentos instalados em unidades de comercialização e dos equipamentos embarcados nos veículos;

ii. Abastecimento de créditos para distribuição *offline* nas unidades de comercialização. Os custos das transmissões de dados serão arcados pela concessionária.

iii. Informações sobre linhas inter e intra área, veículos, horários, trajeto, número de passageiros por veículo, manutenções, localização por GPS dos veículos (geoposicionamento) e status dos veículos junto à ARTESP (em termos de cadastro, vistorias e fiscalizações);

Além da transmissão dos dados, as Concessionárias deverão fornecer *logins* e senhas dos respectivos CCOs para ARTESP. Estes *logins* terão acesso à visualização e *download* de todas as informações.

#### **1.4.2. CCO - Centro de Controle Operacional**

A concessionária deverá implantar, operar e manter sistema de processamento de dados, de controle dos Cartões Inteligentes, cadastros, transações de comercialização, viagens-utilização, monitoramento, atendimento ao usuário, podendo-o realizar em equipamento próprio ou de terceiros. O CCO da Concessionária deverá atender os requisitos de:

- I. Alta confiabilidade;
- II. Alta disponibilidade;
- III. Alta confidencialidade.

Deverão ser garantidos níveis de desempenho compatíveis com o exigido para o desempenho operacional do SIBEM, cabendo salientar a sua grande influência perante a população.

Nível de Serviço do CCO: os equipamentos deverão estar em operação em 99,999% (noventa e nove vírgula novecentos e noventa e nove por cento) do tempo, ou seja, admite-se apenas a inoperância de até 8,760 horas ao ano.

Cada concessionária deverá submeter-se aos níveis descritos na tabela a seguir:

Meta	Forma	Método de coleta	Notificação ao Usuário (min)
Cluster de Servidores	Disponibilidade	Ativo ou Inativo	15
Servidores Web	Disponibilidade	Teste dos serviços	15
Tempo de Manutenção Planejada	Política de Gerenciamento de Mudanças	Relatório de execução da Manutenção	15
Rede interna do CCO	Disponibilidade	Serviço de Echo (PING)	15
Banco de Dados	Disponibilidade	Query no database	15

As bases de dados necessárias para o armazenamento de todas as informações e aplicações do SIBEM, tais como: Cartões Inteligentes, cadastros, transações de viagens, vendas de créditos eletrônicos e outras, bem como as bases utilizadas na administração da segurança do SIBEM (arquivos de chaves dinâmicas e certificados) deverão ser mantidas em segurança, com manutenção de back-ups de acordo com as melhores práticas do setor.

As Bases de Dados deverão ser armazenadas em memórias redundantes de alta confiabilidade e com capacidades suficientes de acordo com as necessidades legais e de informação de cada concessionária.

Todas as informações contidas nas Bases de Dados deverão ser protegidas contra modificações não autorizadas nos diversos níveis de autorização sempre acompanhadas das assinaturas que certificam tais informações como fidedignas, de forma a permitir verificações de autenticidade em eventuais processos de auditoria.

#### **1.4.3. Central de Atendimento**

A concessionária deverá implantar, operar e manter, a Central de Atendimento em consonância com o Decreto Federal nº 6.523, de 31/07/2008, e Lei Estadual nº 10.294, de 20/04/1999, incluindo respectivas regulamentações e normas da ARTESP relacionadas à matéria, sem prejuízo da previsão contratual acerca da implantação de Ouvidoria.

A Central de Atendimento aos usuários deverá operar de acordo com o estabelecido no contrato de concessão, recebendo as comunicações dos usuários por todos os meios de comunicação gratuitamente inclusive, a partir de telefones celulares, referentes a reclamações, sugestões, elogios, pedidos de informações, cadastramentos, pedidos de bloqueios e cancelamento de Cartões Inteligentes. Deverá, também, receber comunicações a partir dos equipamentos de vendas de créditos eletrônicos por autoatendimento, por conexão *online* do usuário: e-mail, *site* eletrônico da concessionária e outras.

Com o *login* e senha do CCO fornecido à ARTESP, esta poderá consultar e fazer *download* de toda e qualquer informação da Central de Atendimento.

#### 1.4.4. Integração entre ARTESP e Operadores

O processo de integração entre ARTESP e concessionárias dar-se-á através da troca segura de informações entre os HSMS (*Hardware Security Module*) das concessionárias e o CCI da ARTESP. A ARTESP terá acesso às Bases de Dados das concessionárias através de canais seguros de comunicação, criados com ajuda dos HSMS. Essas bases de dados deverão conter informações de todas as transações ocorridas de venda e uso de créditos eletrônicos, bem como os dados relativos ao monitoramento da frota.

São obrigações da concessionária:

- I. Garantir a comunicação entre o CCI da ARTESP e os seus HSMS;
- II. Manter os HSMS, locados em seu Data Center, em perfeito funcionamento, garantindo sua perfeita manutenção.

Detalhes dos processos de segurança serão apresentados no item *Sistema de Bilhetagem e Monitoramento*.

#### 1.5. Auditoria

O SIBEM deverá possuir rotinas automáticas de auditorias que validem a integridade de todos seus processos, como por exemplo, a consistência do saldo de um Cartão Inteligente com a sua movimentação de débito e crédito.

As rotinas de auditoria deverão definir mecanismos automáticos e procedimentos associados que registrem todas as atividades importantes do SIBEM.

Algumas características destas rotinas são:

- I. Registro de atividades relevantes, isto é, quaisquer atividades que possam potencialmente estar relacionadas com algum tipo de ataque;
- II. O esquema de auditoria deverá causar o menor impacto possível sobre as rotinas normais do SIBEM, não causando impacto em desempenho e disponibilidade;
- III. A informação de auditoria deverá ser armazenada de maneira uniforme e com facilidade de acesso na consulta e interpretação;
- IV. A informação de auditoria deverá ser protegida contra ataques;
- V. A identificação e a autenticação estão relacionadas às rotinas de auditoria. O SIBEM deverá ser capaz de identificar corretamente a entidade responsável por operação registrada;
- VI. O SIBEM deverá manter uma base de dados sobre operações realizadas e respectivas participações de entidades, permitindo o exame específico das ações de uma ou mais entidades. Os dados da base de dados do SIBEM deverão estar sempre acompanhados de assinaturas criadas em tais operações, que certificam a autenticidade desses dados. Essas assinaturas deverão ser geradas com auxílio de HSMS (*Hardware Security Module*) instalados no CCO das concessionárias.

A ARTESP irá definir procedimentos específicos de auditoria e realizá-los por meios próprios ou por terceiros contratados, quando julgar necessário.

### **1.6. Contingência**

A concessionária deverá desenvolver um plano de contingência do SIBEM, considerando as diretrizes abaixo relacionadas e submetê-lo à apreciação e aprovação da ARTESP. O plano de contingência, após aprovado, deverá ser implementado junto com o SIBEM.

O plano de contingência do SIBEM deverá prever todas as ações e medidas para pronta realização, com vistas a assegurar a continuidade dos processos nos casos de ocorrência anormal com perda ou deterioração nos serviços, cujas consequências possam provocar prejuízos ou sérios danos a pessoas ou a bens patrimoniais da própria concessionária, dos usuários, da ARTESP ou de terceiros.



Tudo que apresenta potencial de gerar uma ocorrência anormal deve constar no plano de contingência do SIBEM, com respectivas ações e medidas preventivas.

O plano de contingência deverá, também, definir as responsabilidades, estabelecer organização para atender a uma emergência e conter informações detalhadas sobre as características da ocorrência anormal. Deverá ser desenvolvido curso entre todos os funcionários da concessionária com o intuito de treinar, organizar, orientar, facilitar, agilizar e uniformizar as ações necessárias às respostas de controle e combate às ocorrências anormais (planejamento de riscos e de recuperação de desastres).

Deverá, ainda, descrever as medidas a serem tomadas, incluindo a ativação de processos manuais, para fazer com que seus processos vitais voltem a funcionar plenamente, ou num estado minimamente aceitável, o mais rápido possível, evitando assim uma paralisação prolongada que possa gerar maiores prejuízos, como perdas de dados, informações e de receitas, sanções governamentais e problemas judiciais.

Seus itens deverão estar documentados e a atualização desta documentação deve ser feita sempre que necessário. Testes periódicos no plano também são necessários para verificar se o processo continua válido. O detalhamento das medidas deverá ser o necessário e suficiente para a sua rápida execução.

O plano de contingência deverá conter:

- I. Identificação dos riscos e definição de cenários possíveis de falha para cada um dos processos críticos, levando em conta a probabilidade de ocorrência de cada falha, provável duração dos efeitos, consequências resultantes e os limites máximos aceitáveis de permanência da falha, sem a ativação da respectiva medida de contingência;
- II. Identificação das medidas para cada falha, ou seja, listagem das medidas a serem postas em prática, caso a falha aconteça, incluindo comunicação à própria concessionária, aos usuários, à ARTESP e até mesmo à imprensa;
- III. Definição das ações necessárias para operacionalização das medidas cuja implantação dependa da aquisição de recursos físicos e/ou humanos;
- IV. Implantação de alguma forma de monitoramento que possibilite a rápida atuação em casos anormais, com critérios claros de ativação do plano.

Todos os funcionários da concessionária devem estar familiarizados com o plano, visando evitar hesitações ou perdas de tempo que possam causar maiores problemas em situação de crise.

A concessionária será a responsável por todo eventual prejuízo gerado pela falta da contingência, ou pelo atraso de sua implementação.

A concessionária deverá descrever como executará os serviços quando ocorrerem contingências envolvendo quaisquer dos processos, como por exemplo: ataques de intrusão, constatação de fraudes, usos indevidos do sistema, quebra de segurança dos cartões, módulos de segurança de acesso (chips SAM), chaves privadas, criptografia, senhas, software, ocorrência de paralisações de funcionários, etc.

Deverá, ademais, prever redundâncias para manter os níveis de serviço no que se refere a:

- I. Confiabilidade e disponibilidade das redes de comunicações citadas no item 1.4.1;
- II. Confiabilidade e disponibilidade dos servidores do CCO da concessionária;
- III. Confiabilidade e disponibilidade dos HSMs instalados no CCO da concessionária;
- IV. Confiabilidade e disponibilidade dos equipamentos instalados nas unidades de comercialização e nos veículos.

O Sistema deverá conter uma análise de suas vulnerabilidades, uma lista de possíveis ameaças associadas a essas vulnerabilidades, uma análise dos riscos operacionais associados a cada uma dessas ameaças, bem como um plano de mitigação de riscos operacionais.

Os principais eventos de risco operacional são:

- I. Fraudes internas;
- II. Fraudes externas;
- III. Demandas trabalhistas e segurança deficiente do local de trabalho;
- IV. Práticas inadequadas relativas a clientes, produtos e serviços;

- V. Danos a ativos físicos próprios ou em uso pela instituição;
- VI. Eventos que acarretam a interrupção das atividades da instituição;
- VII. Falhas em sistemas de tecnologia da informação;
- VIII. Falhas na execução, cumprimento de prazos e gerenciamento das atividades na instituição.

O gerenciamento do risco operacional deve prever:

- I. Identificação, avaliação, monitoramento, controle e mitigação do risco operacional;
- II. Documentação e armazenamento de informações referentes às perdas associadas ao risco operacional;
- III. Elaboração, com periodicidade mínima anual, de relatórios que permitam a identificação e correção tempestiva das deficiências de controle e de gerenciamento do risco operacional;
- IV. Realização, com periodicidade máxima anual, de testes de avaliação dos sistemas de controle de riscos operacionais implementados;
- V. Elaboração e disseminação da política de gerenciamento de risco operacional ao pessoal da instituição, em seus diversos níveis, estabelecendo papéis e responsabilidades, bem como as dos prestadores de serviços terceirizados;
- VI. Existência de plano de contingência contendo as estratégias a serem adotadas para assegurar condições de continuidade das atividades e para limitar graves perdas decorrentes de risco operacional;
- VII. Implementação, manutenção e divulgação de processo estruturado de comunicação e informação;
- VIII. Estrutura de gerenciamento do risco operacional capacitada a identificar, avaliar, monitorar, controlar e mitigar os riscos, inclusive decorrente de serviços terceirizados.

Os procedimentos de contingência devem incluir:

- I. Manutenção de back-up regular das bases de dados;
- II. Manutenção de um “*site* de contingência” sempre atualizado;
- III. Imagens completas e atualizadas de servidores vitais para o funcionamento (principalmente os que requerem muito tempo para reconstituição);
- IV. Manutenção de senhas em local seguro, mas de fácil acesso às pessoas autorizadas no caso de uma emergência;
- V. Profissionais preparados para atuação imediata;
- VI. Hardware redundante.

Além disso, o SIBEM deverá ser dotado de recursos que permitam:

- I. Contingência de energia elétrica desejável de pelo menos 2 horas, para o funcionamento dos equipamentos de recarga de Cartões Inteligentes instalados nas bilheterias de terminais e rodoviárias;
- II. Contingência de comunicação com o CCO da concessionária para o funcionamento dos equipamentos de recarga de Cartões Inteligentes instalados nas bilheterias de terminais e rodoviárias;
- III. Rápida troca de chaves ou algoritmos de criptográficos dos HSMs e Módulos de Segurança de Acesso (SAM), no caso de quebra da segurança.

## **2. Sistema de Bilhetagem e Monitoramento**

O SIBEM Sistema Integrado de Bilhetagem Eletrônica e Monitoramento, apresentado neste item, deverá estar implementado conforme descrito a seguir.

### **2.1. Processos Suportados**

- I. Adquirir, inicializar, personalizar e distribuir os Cartões Inteligentes para acesso aos veículos pertencentes aos serviços rodoviários intermunicipais de transporte coletivo de passageiros no Estado de São Paulo;

- II. Adquirir, instalar e manter os Módulos de Segurança de Acesso (chips SAM) em todos os equipamentos definidos neste Termo de Referência;
- III. Gerar, distribuir e comercializar créditos eletrônicos monetários para carga nos Cartões Inteligentes;
- IV. Adquirir, instalar, manter e controlar os equipamentos de recarga, terminais de vendas (PDVs) e máquinas de autoatendimento, para utilização nos pontos de comercialização de créditos pertencentes ao SIBEM;
- V. Gerir e controlar a efetivação das cargas nos equipamentos de recarga e nos Cartões Inteligentes, decorrentes das autorizações de carregamento pré-pagos (listas de recarga);
- VI. Adquirir, instalar, manter e controlar os validadores para utilização nos veículos pertencentes ao SIBEM;
- VII. Adquirir, instalar, manter, gerir e controlar as catracas de ônibus;
- VIII. Adquirir, instalar, manter, gerir e controlar a conectividade e comunicação de dados entre todos os equipamentos do sistema e a ARTESP;
- IX. Capturar e arquivar todos os dados gerados pelo SIBEM;
- X. Processar todas as transações geradas pelo sistema, incluindo a disponibilização das mesmas para a ARTESP;
- XI. Cumprir solicitações da ARTESP referente as alterações no sistema, visando atender políticas tarifárias e alterações nas regras de negócio;
- XII. Implantar o processo de alteração das regras e parâmetros de tarifação do SIBEM;
- XIII. Cadastrar os usuários responsáveis e titulares de Cartões Inteligentes, inclusive de escolares e de gratuidades;
- XIV. Implantar e operar centrais de atendimento e postos de atendimento para atender ao público;

- XV. Fornecer Cartões Inteligentes para os usuários (inclusive para beneficiários de isenções totais e parciais de tarifação no acesso ao sistema, de acordo com a legislação vigente);
- XVI. Gerenciar as listas de Cartões Inteligentes irregulares;
- XVII. Adquirir, instalar, manter, gerir e controlar os DGCs - Dispositivos de Geoposicionamento e Comunicação, que serão utilizados nos veículos;
- XVIII. Adquirir, instalar, manter, gerir e controlar os displays, que serão utilizados nos terminais rodoviários, como parte do sistema de informação ao usuário;
- XIX. Adquirir, instalar, manter, gerir e controlar os contadores de passageiros, que serão utilizados nos veículos;
- XX. Adquirir, instalar, manter e controlar equipamentos para implantação de CCO da concessionária, formado por servidores e HSMS que permitam executar funcionalidades de comunicação e troca de dados com equipamentos, disponibilização de dados e comunicação com CCO da ARTESP, processamento e verificação de autenticidade de transações de venda de créditos, de viagens, utilização de créditos e de monitoramento de frota;
- XXI. Disponibilizar para a ARTESP todas as transações diárias realizadas no CCO da concessionária.

### **3. Transações / Processos Sistêmicos**

#### **3.1.1. Processos Comuns ao Rodoviário e Suburbano**

Em decorrência da premissa do Cartão Inteligente ser único para ambas as modalidades, rodoviária e suburbana, os processos descritos a seguir são únicos.

## Sistema de Cadastro de Usuários

A criação e manutenção da base de usuários que deverá ser utilizada para emissão de Cartões Inteligentes “**personalizados**” ou “**identificados**” é de responsabilidade da Concessionária.

Os cartões “**personalizados**” serão destinados para passageiros com gratuidade ou escolar. Os cartões personalizados podem habilitar usos múltiplos em um mesmo cartão, desde que sob o cadastro de um mesmo usuário (uso como VT, escolar e comum concomitantemente, por exemplo). Os cartões personalizados são os que apresentam nome e fotografia do usuário.

Os cartões “**identificados**” serão destinados para os demais usuários e apresentam apenas uma identificação que associa o cartão ao seu titular. Os cartões identificados podem habilitar usos múltiplos em um mesmo cartão, desde que sob o cadastro de um mesmo usuário (como VT e comum concomitantemente, por exemplo).

Estes cadastros poderão ser realizados em unidades de atendimento (física) na Concessionária, ou através de *site* eletrônico disponibilizado pela Concessionária.

Por *login* e senha do SIBEM fornecido à ARTESP, esta poderá consultar e fazer *download* de toda e qualquer informação do Sistema de Cadastro de Usuários.

O Sistema de Cadastro de Usuários é responsável por:

### I. Cadastro de Empresas Adquirentes de Vale Transporte

Para viabilizar a comercialização de créditos eletrônicos de VT - Vale Transporte, deverão ser realizados os seguintes cadastros:

- Cadastro de Credenciadas;
- Cadastro de empregadores: Pessoa física ou Jurídica.

A associação do beneficiário com um Cartão Inteligente poderá ser realizada pela concessionária ou pelas credenciadas, decorrente de negociações efetuadas entre as mesmas.

Após efetuar o seu cadastro, a empresa empregadora deverá cadastrar também os seus empregados.

## II. Cadastro de Escolas

É o cadastro contendo as informações das escolas e respectivos cursos, de ensino: fundamental, médio, superior e profissionalizante, das redes pública e privada de ensino, responsáveis pelas informações contidas em formulário de solicitação do benefício do cartão escolar.

## III. Cadastro de Usuários

A criação e manutenção de uma base de usuários, utilizada para emissão de cartões personalizados ou identificados, é de responsabilidade da Concessionária.

Os locais de atendimento aos usuários são de responsabilidade das Concessionárias.

O cadastro de usuários está subdividido em:

- 1) Vale Transporte:** é o cadastro dos empregados (beneficiários) das empresas adquirentes de Vale Transporte;
- 2) Comum:** é o cadastro de usuários que comprem antecipadamente créditos monetários e não são beneficiados com desconto ou gratuidade no pagamento da tarifa. O cadastro pode ser realizado nas Unidades de Atendimento ou via Internet. A confecção do Cartão Inteligente pode ser realizada no momento do cadastramento, caso o mesmo ocorra em uma das unidades de atendimento (bilheterias ou garagens) ou de forma centralizada, sendo enviado ao usuário.
- 3) Escolar:** é o cadastro dos estudantes e professores, beneficiados pela redução de 50% do valor da tarifa. O estudante ou professor poderá ser cadastrado quando recebida a comunicação da Escola. O sistema deverá permitir importação de arquivo de texto contendo os dados dos estudantes matriculados, bem como arquivos de fotos. Esta informação será utilizada para a inicialização e personalização dos cartões.

Um mesmo usuário pode estar cadastrado em múltiplas categorias. Consequentemente, os Cartões Inteligentes devem possibilitar usos múltiplos em um mesmo cartão (vale transporte, comum, escolar e suas combinações).



O cadastramento do estudante ou professor poderá ser realizado nas bilheterias ou garagens das concessionárias, apresentando o comprovante de matrícula e comprovante de residência.

A concessão deste benefício está oficializada nas regras tarifárias previstas no Anexo V – Política Tarifária.

**4) Gratuidades:** Conforme legislação vigente até a data de publicação do Edital e regras previstas no Anexo V – Política Tarifária.

A validade do benefício gratuidade é gravada nos cartões pertencentes aos usuários que possuem este direito, sendo de responsabilidade do consórcio a validação legal (comprovação pelos usuários com as respectivas documentações) do direito ao benefício, bem como a atualização do benefício no Cartão Inteligente.

Os Cartões Inteligentes gratuidade e escolar são personalizados com a foto do usuário.

Os Cartões Inteligentes possuem um período de validade, sendo:

- Validade de 2 anos, para os casos de incapacidade definitiva e aposentadoria por invalidez;
- Pelo período indicado no parecer médico como necessário ao tratamento, limitado ao prazo de máximo de 1 ano, para os casos de incapacidade temporária, com possibilidade de renovação.
- Validade de 5 (cinco) anos para o usuário gratuidade idoso.

Todos os períodos de validade deverão ser configuráveis através de parâmetros do sistema.

### **Emissão de Cartão Inteligente**

É de responsabilidade da Concessionária a aquisição, emissão e distribuição do Cartão Inteligente para todos os tipos de usuários, inclusive gratuidade, em conformidade com o Padrão definido pela ARTESP.

## **Cancelamento de Cartão Inteligente**

Em caso de perda, roubo ou danificação do cartão, o mesmo poderá ser cancelado junto à Concessionária, gerando um protocolo, que poderá ser utilizado para aquisição de um novo cartão e uma restituição de créditos eletrônicos existentes.

Os cartões cancelados serão informados de forma *online* aos veículos, atualizando uma lista restritiva.

## **Bloqueio e Desbloqueio de Cartão Inteligente**

Deverão ser implementadas transações de bloqueio e respectivo desbloqueio no uso de Cartões Inteligentes para os casos em que justifique este tipo processo, tal como, envio de Cartões Inteligentes pelo correio e perda temporária.

## **Listas Restritivas**

Os cartões cancelados deverão ser transferidos para os validadores dos veículos para que, uma vez apresentados em qualquer validador, sejam inutilizados.

## **Restituição de Créditos Eletrônicos no Cartão Inteligente**

Para os cartões cancelados e que possuam saldo, a partir do momento em que o usuário efetuou o cancelamento junto ao sistema da concessionária, o sistema deverá calcular o saldo a ser restituído, deixando este valor disponível para ser gravado em novo cartão ou ser diretamente restituído para o cliente.

Ao final do período de 1 (um) ano sem que ocorra qualquer movimentação no cartão, os clientes deverão ser informados que possuem saldo.

Os créditos adquiridos no sistema e não utilizados por um período de 1 (um) ano serão revertidos à ARTESP.

## **Consultas de Saldos**

Deverão ser disponibilizados equipamentos para consultas de saldos existentes em Cartões Inteligentes dos usuários nos terminais (bilheterias), pontos de vendas (rodoviárias), pontos de vendas de redes, etc. Os saldos também poderão ser consultados pela internet.

## Auditoria

O sistema SIBEM deverá ser aberto e disponível para auditorias a qualquer tempo, a critério da ARTESP.

### a. Controle de saldos de créditos eletrônicos

Para cada Cartão Inteligente deverá ser mantido no SIBEM, uma conta corrente contendo todas as viagens-utilização (débitos), as recargas realizadas (créditos) e o saldo atualizado. Todos os registros de viagens-utilização e recargas realizadas deverão ser verificados, quanto a sua autenticidade, e armazenados em banco de dados do SIBEM, acompanhados da assinatura eletrônica que os autentica.

A Concessionária deverá informar a ARTESP o saldo de créditos eletrônicos em Cartões Inteligentes em poder dos usuários.

### b. Controle e responsabilidade de saldos de créditos eletrônicos negativos - Cartões Inteligentes

Em decorrência do Cartão Inteligente do usuário habitual eventualmente possuir saldo negativo, quando da complementação do saldo existente no cartão, o saldo negativo será compensado na próxima recarga.

A Concessionária arcará com o saldo negativo não recuperado em recarga.

## Geração de Informações para os displays do Sistema de Informação (Rodoviárias e Terminais)

A Concessionária deverá apresentar as informações atualizadas em determinados intervalos de tempo, contendo:

- I. Próximas partidas (horário e plataformas de embarque);
- II. Próximas chegadas (horário e plataformas de desembarque);
- III. Informações institucionais

## Consulta de Informações

A Concessionária deverá disponibilizar a consulta de informações sobre os serviços rodoviários intermunicipais de transporte coletivo de passageiros, entre elas:

- I. Ligações e itinerários;
- II. Horários;
- III. Tarifas;

Essas informações deverão estar disponíveis em vários canais:

- I. Sítio eletrônico - Internet;
- II. Máquinas de autoatendimento;
- III. Bilheterias;
- IV. Telefone;
- V. Outros canais, que serão viabilizados em decorrência da evolução da tecnologia.

### 3.1.2. Processos da Modalidade Suburbana

Na modalidade suburbana a forma de tarifação é segmentada, ou seja, o usuário paga a passagem correspondente ao trecho viajado.

A viagem deverá ser viabilizada tanto para os usuários que possuem um Cartão Inteligente, denominados usuários habituais, que poderão ser do tipo: comum, estudante, vale-transporte, etc., ou para usuários que não possuem um Cartão Inteligente, denominados usuários eventuais, que efetuam o pagamento da viagem em dinheiro, na bilheteria ou ao condutor do veículo.

Um mesmo cartão de usuário habitual pode possuir um ou mais tipos de produtos: VT e comum, estudante e comum, etc.

## Vendas de Créditos Eletrônicos

A venda de créditos eletrônicos deverá ser realizada em unidades de comercialização da própria Concessionária (rede própria) ou por terceiros credenciados e subcontratados (redes de terceiros):

- I. Rede própria - Bilheterias de terminais, estações rodoviárias e garagens;
- II. Redes de terceiros - Estabelecimentos externos aos Terminais e Rodoviárias;

Quanto ao tipo de atendimento deve-se ter:

- I. Atendente, em equipamentos assistidos;
- II. Máquinas de autoatendimento, operados diretamente pelos próprios usuários;
- III. Sítio de comércio eletrônico (Internet);
- IV. Eventualmente outros, como ATM bancário, etc.

Todos os equipamentos que efetuam venda de créditos deverão ter um chip SAM instalado que permita realizar com segurança as funções de acesso e atualização de dados dos Cartões inteligentes.

Os equipamentos assistidos e de autoatendimento deverão realizar o processo de recarga de créditos mediante autorização de um elemento seguro, que disponha de créditos para transferência aos cartões inteligentes.

O dispositivo de segurança e de armazenamento de créditos poderá ser:

- O HSM instalado no CCO da Concessionária, acessível *online* pelo equipamento através de rede de comunicação com o Servidor de Recarga do SIBEM; ou
- O SAM instalado no equipamento, enquanto existir saldo disponível de créditos para distribuição.

Para distribuição de créditos *offline*, isto é, através do chip SAM, os equipamentos instalados nas unidades de comercialização deverão realizar operações *online* de abastecimento de créditos, acessando, via rede de comunicação, o Servidor de Recarga do SIBEM.

As funções básicas a serem desempenhadas pelas unidades de comercialização são:

- I. Fornecimento de Cartão Inteligente;
- II. Fornecimento de Cartão Inteligente para viagem unitária;
- III. Cadastramento de usuários, inicialização e personalização de Cartões Inteligentes;
- IV. Carga do Cartão Inteligente com créditos eletrônicos, com auxílio do HSM (recarga *online*) ou do chip SAM (recarga *offline*);
- V. Verificação de dados armazenados no Cartão Inteligente (prazo de validade, titular e saldos), com auxílio do chip SAM;
- VI. Registro de operações de recarga, acompanhadas de assinatura eletrônica gerada pelo chip SAM;
- VII. Transmissão de transações de recarga realizadas;
- VIII. Atualização automática de parâmetros e versões de software dos equipamentos de venda de créditos, mediante conexão *online* com o Servidor de Recarga do SIBEM;
- IX. Recebimento do numerário referente ao valor da venda dos créditos eletrônicos, ou pagamento via cartão de débito ou crédito;
- X. Fornecimento de troco ao usuário (cédulas e moedas metálicas) quando da venda de créditos eletrônicos;
- XI. Fornecimento de recibo;
- XII. Eventual reembolso.

### **Vendas de Créditos Eletrônicos - Usuários Habituais (possuem Cartão Inteligente)**

Os créditos eletrônicos poderão ser adquiridos pelos usuários habituais em diversos canais: máquinas de autoatendimento e terminais de venda em bilheterias, pagos e carregados no Cartão Inteligente.

O sistema deverá emitir o cupom fiscal que permita a comprovação da despesa correspondente à aquisição ou carregamento de cartões.

O Cartão Inteligente constante na lista restritiva não poderá ser recarregado.

Tanto a transação de recarga quanto a transação de bloqueio do Cartão Inteligente deverão ser assinadas utilizando módulo SAM e informada à ARTESP.

### **Vendas de Créditos Eletrônicos - Usuários Habituais - Estudante**

Os créditos eletrônicos para usuários do tipo estudante poderão ser adquiridos em diversos canais: máquinas de autoatendimento e terminal de vendas em bilheterias, pagos e carregados no Cartão Inteligente.

O estudante terá um limite mensal de compra determinado pelo deslocamento entre a residência e a escola. Este poderá efetuar compras de créditos eletrônicos parciais, dentro deste limite.

O cartão do estudante constante na lista restritiva não poderá ser recarregado.

Tanto a transação de recarga quanto a transação de bloqueio do Cartão do Estudante deverá ser assinada utilizando módulo SAM e informada à ARTESP.

### **Vendas de Créditos Eletrônicos - Usuários Eventuais (não possuem Cartão Inteligente)**

Os créditos eletrônicos em Cartões Inteligentes do tipo “viagem unitária” serão adquiridos pelos usuários eventuais junto ao operador, utilizando o terminal de dados acoplado ao validador de entrada. A tarifa será calculada de acordo com a informação das coordenadas do ponto de origem fornecidas pelo Dispositivo de Geoposicionamento e Comunicação e com a informação do ponto de destino fornecido pelo condutor. O valor destes créditos eletrônicos será pago ao condutor em dinheiro e serão gravados no Cartão Inteligente de viagem unitária.

Poderá ser efetuada a venda de passagem unitária para usuários eventuais em cartões de viagem unitária, em bilheterias da Concessionária (rede própria ou de terceiros), através da informação do passageiro do ponto de destino.

Esta transação deverá ser assinada utilizando módulo SAM e informada à ARTESP.

## **Vendas de Créditos Eletrônicos para Recargas Pré-Pagas (lista)**

Os créditos eletrônicos poderão ser adquiridos e pagos previamente por PF (Pessoas Físicas) ou PJ (Pessoas Jurídicas) e disponibilizados para recarga para os usuários habituais em diversos canais: máquinas de autoatendimento, terminal de vendas em bilheterias e no validador de entrada a bordo do ônibus.

A forma mais comum de utilização deste processo é o VT - Vale Transporte adquirido por empresas para disponibilização para seus funcionários.

O atendimento a empresas referente à recarga de VT - Vale Transporte, deverá ser negociado diretamente entre as empresas e a Concessionária.

O sistema deverá permitir a emissão de cupom fiscal que permita a comprovação da despesa correspondente à aquisição ou carregamento de cartões.

Tanto a transação de recarga quanto a transação de bloqueio de Cartão VT deverão ser assinadas utilizando módulo SAM e informada à ARTESP.

## **Recargas de Créditos Eletrônicos por Lista - Usuários Habituais (possuem Cartão Inteligente)**

Os créditos eletrônicos adquiridos e pagos previamente poderão ser carregados pelos usuários habituais em diversos canais: máquinas de autoatendimento, terminal de vendas em bilheterias e no validador de entrada do ônibus.

O Cartão Inteligente constante na lista restritiva não poderá ser recarregado.

Tanto a transação de recarga quanto a transação de bloqueio do Cartão Inteligente deverão ser assinadas utilizando módulo SAM e informada à ARTESP.

## **Viagem - Utilização**

O processo de Viagem-Utilização contempla a cobrança da tarifa para o acesso ao transporte, realizando o débito no Cartão Inteligente e a liberação de passagem pela catraca.



Contempla, também, a verificação de direito e validade para acesso ao transporte Cartão Inteligente Especial (gratuidades) e a liberação de passagem pela catraca.

Existem dois validadores instalados nos veículos suburbanos, um junto à porta de acesso e outro junto à catraca na porta de saída.

A concessionária deverá manter controle de todos os validadores e dos módulos de segurança de acesso (chips SAM) neles instalados, responsabilizando-se pelos riscos de fraudes, falhas e disponibilidade ao uso desses equipamentos.

As informações geradas nas transações de Viagem-Utilização deverão ser assinadas utilizando módulo SAM e transmitidas e armazenadas no SIBEM.

Nos validadores serão registrados os parâmetros do sistema, a estrutura tarifária e a lista restritiva (cartões irregulares) para evitar a utilização de Cartões Inteligentes com irregularidades.

A inclusão de Cartões Inteligentes na lista restritiva deverá ser realizada de forma *online*.

As principais funções dos equipamentos de validação no controle de acesso e tarifação devem ser:

- I. Leitura e processamento das informações contidas no Cartão Inteligente, com auxílio do módulo SAM, indicando ao usuário a validade ou problemas existentes no Cartão Inteligente, mediante um visor de informações (display);
- II. Acionar o controle da catraca permitindo ou não a liberação da saída segundo o resultado do processamento do Cartão Inteligente;
- III. Manter ativa a autorização de passagem, após considerar válida a autorização de passagem e cancelá-la automaticamente somente após a passagem do usuário pela catraca, sendo que a autorização de passagem não poderá ser cancelada por quaisquer outros motivos, inclusive por mudança de estado operacional;
- IV. Evitar que o direito de viagem de um Cartão Inteligente válido seja cancelado pela utilização incorreta por parte do usuário imediatamente anterior, como, por exemplo, por movimentação incompleta da barreira (curso parcial);

- V. Apresentação para o usuário e/ou operador de informação pictográfica de existência de alarme e passagem sujeita a fiscalização;
- VI. Apresentação de informação visual e acústica de rejeição do Cartão Inteligente, indicação de passagem liberada, de valor debitado, de saldo, solicitação de reapresentação do cartão e outras;
- VII. O software executável do validador deverá ser auditável, ou seja, depois de homologado, aprovado, instalado e em funcionamento nos validadores deverá ser possível a concessionária verificar, mediante comparação com cópia autenticada, se houve qualquer alteração no software executável em operação.
- VIII. Deverá ser feita verificação periódica, automática e rápida da versão do software executável, através da quantidade de bytes e/ou assinatura eletrônica.
- IX. Os validadores deverão suportar operação ininterrupta 24 horas por dia, todos os dias do ano.
- X. O validador além de validar as informações no Cartão Inteligente autorizando a utilização do transporte pelo usuário deverá executar a gravação de informações e a captura dos dados de transação e, no caso da passagem tarifada, o débito da tarifa correspondente. Estas informações deverão ser enviadas ao sistema de bilhetagem eletrônica da concessionária.
- XI. Atualizar-se com novas versões de parâmetros e listas restritivas somente após aferir a confiabilidade destas informações mediante verificação pelo módulo SAM;
- XII. Garantir a segurança das transações utilizando o módulo SAM como mecanismo confiável para:
- a. Verificação de autenticidade dos dados dos cartões inteligentes;
  - b. Execução de operações seguindo uma máquina de estados que garante um ciclo seguro de operações;
  - c. Atualização de saldo e dados de viagens do cartão, mantendo integridade dos mesmos;

- d. Geração de assinaturas eletrônicas que autenticam as transações.

XIII. O validador deverá gravar as informações referentes a outros eventos como:

- a. Transações individualizadas de cada Cartão Inteligente, contendo no mínimo as seguintes informações: número lógico do Cartão Inteligente, tipo de Cartão Inteligente, data e hora da transação, prefixo do veículo, ligação, modalidade (rodoviária ou suburbana), tipo de transação (débito, gratuidade), ponto de origem, ponto de destino, tipo de tarifa, valor debitado, assinatura da transação.
- b. Cartões Inteligentes irregulares, com código do motivo da recusa;
- c. Ocorrências de falhas durante a operação;
- d. Cartões Inteligentes cancelados por constarem na lista restritiva;
- e. Horários de início e fim de serviços e meias viagens;
- f. Cartões Inteligentes bloqueados;
- g. Gerenciamento de informações armazenadas no validador, tais como parâmetros, lista restritiva de Cartões Inteligentes, lista de recarga de Cartões Inteligentes, tarifas, novas versões de software do próprio validador, etc.

#### **Utilização - Usuários Habituais (possuem Cartão Inteligente)**

O Cartão Inteligente é apresentado no validador existente na entrada do veículo, sendo debitado o valor cheio da tarifa e registrado no cartão o ponto de origem correspondente à coordenada levantada pelo Dispositivo de Geoposicionamento e Comunicação.

No ponto de destino, identificado pela apresentação do Cartão Inteligente e através da coordenada levantada com auxílio do Dispositivo de Geoposicionamento e Comunicação, o validador de saída efetuará o cálculo da tarifa a ser debitada no cartão do usuário, comparando o ponto de origem com o ponto de destino. O validador efetuará o respectivo débito, liberando em seguida a catraca.

As informações referentes a esta viagem deverão ser repassadas para o sistema Central da Concessionária, de forma *online*, e disponibilizada para busca pela ARTESP.

Na condição do cartão não possuir saldo suficiente para pagamento da tarifa calculada, a catraca de saída será liberada, possibilitando assim o usuário completar a sua viagem. O cartão ficará com um saldo negativo que será compensado na próxima recarga efetuada pelo usuário.

Caso ocorra alguma situação em que o GPS não consiga determinar a coordenada de forma adequada, o condutor informará, via Terminal de Dados, o ponto de origem ou de destino.

Esta transação deverá ser assinada utilizando módulo SAM e informados à ARTESP.

### **Utilização - Usuários Eventuais (não possuem Cartão Inteligente)**

Para os usuários que não possuem o seu Cartão Inteligente, será utilizado um cartão de viagem unitária, onde o usuário informará o seu destino ao condutor que registrará esta informação no sistema. O sistema efetuará o cálculo do valor da passagem a ser pago pelo passageiro ao condutor e gravará o direito a esta viagem no cartão de viagem unitária, que será entregue ao passageiro.

No destino, o usuário apresentará o cartão no validador de saída que efetuará a validação do ponto de destino (levantamento da coordenada GPS com auxílio do Dispositivo de Geoposicionamento e Comunicação) onde foi apresentado o cartão e o ponto de destino informado pelo o usuário no momento da entrada no veículo.

Caso o valor da passagem paga corresponda ao trecho da viagem, a catraca de saída será liberada e o validador de saída efetuará o recolhimento do cartão viagem unitária.

Caso o valor da passagem seja menor que o valor correspondente ao trecho de viagem, o passageiro terá que pagar o valor complementar ao condutor, que atualizará as informações no cartão viagem unitária possibilitando a apresentação e recolhimento do cartão viagem unitária, e a respectiva liberação da catraca de saída.

Esta transação deverá ser assinada utilizando módulo SAM e informada à ARTESP.

### **Utilização - Gratuidades**

Os usuários que possuem direito à gratuidade, tais como idosos, pessoas com deficiência, possuirão um Cartão Inteligente especial, personalizado e com data de validade, de acordo com o tipo de gratuidade.

Para os usuários que não possuam o Cartão Inteligente próprio e apresentem a identidade para validação da condição de idoso, deverá o condutor informar a situação à concessionária e promover a entrada do usuário ao veículo.

Esta transação deverá ser assinada utilizando módulo SAM e informada à ARTESP.

Em linhas suburbanas com tarifa única, poderá a concessionária configurar a sua frota com uma catraca e um validador na entrada do veículo.

Em linhas suburbanas multi-tarifas, poderá a concessionária, configurar a sua frota com duas catracas e dois validadores nas portas de embarque e desembarque, desde que não restrinja o acesso aos cadeirantes.

### **Utilização - Estudantes e Professores**

Os usuários serão caracterizados como estudante/professor, com Cartão Inteligente personalizado e com fotografia.

A entrada e saída deverão ser assinadas utilizando módulo SAM e informada à ARTESP.

### **Emissão de Cartão Inteligente - Operacionais**

É de responsabilidade da concessionária a aquisição, emissão e controle dos Cartões Inteligentes operacionais para:

- I. Identificação do condutor (abertura e fechamento de serviços);
- II. Inicialização das ligações;
- III. Identificação de fiscais.

Os cartões de identificação dos condutores e fiscais deverão ser personalizados.

### **Inicialização de ligações**

O processo de associação da ligação a um determinado veículo (prefixo do veículo), quando do início de operação ou mudança da ligação durante a operação deverá ser realizada por um fiscal de linha ou supervisor na garagem, utilizando um Cartão Inteligente, com tal função, onde no mesmo estaria gravada a ligação.

A verificação da autenticidade do Cartão Inteligente do fiscal de linha ou supervisor e a geração de assinatura para a transação de inicialização da ligação serão realizadas através de módulo SAM. Esta transação deverá ser informada à ARTESP.

As informações deverão ser enviadas *online* para o CCO da Concessionária e para o SIBEM.

### **Abertura de Serviço**

No início de um turno de operação por um condutor, o mesmo deverá efetuar o seu *login*, utilizando o seu Cartão Inteligente e informar ao sistema o início da operação (saída da garagem) e/ou do turno.

No instante em que o veículo é ligado, todos os componentes embarcados são ligados e o validador de entrada estabelece o sincronismo com os mesmos, possibilitando assim o início da operação.

A verificação da autenticidade do Cartão Inteligente do condutor e a geração de assinatura para a transação de abertura de serviço serão realizadas através de módulo SAM. Esta transação deverá ser informada à ARTESP.

As informações deverão ser enviadas *online* para o CCO da Concessionária e para o SIBEM.

### **Fechamento de Serviço**

No final de um turno de operação por um condutor, o mesmo deverá efetuar o seu *login*, utilizando o seu Cartão Inteligente e informar o final de uma operação (retorno para a garagem) e/ou do turno.

A verificação da autenticidade do Cartão Inteligente do condutor e a geração de assinatura para a transação de fechamento de serviço serão realizadas através de módulo SAM. Esta transação deverá ser informada à ARTESP.

As informações deverão ser enviadas *online* para o CCO da Concessionária e para o SIBEM.

## Contagem de Passageiros

Em todo ponto de parada, serão contabilizados os passageiros que entraram no veículo e os passageiros que saíram, gerando um evento que será enviado ao CCO da concessionária.

Esta transação deverá ser assinada utilizando módulo SAM e informada à ARTESP.

Para a modalidade suburbana, estas informações serão obtidas dos validadores de entrada e saída do veículo.

### 3.1.3. Processos da Modalidade Rodoviária

Em decorrência das características específicas da forma de tarifação, estão descritos abaixo, os requisitos de negócio específicos desta modalidade.

#### Vendas de Passagens - Bilheterias

A transação de venda de passagens da modalidade rodoviária, quando da utilização de cartão inteligente para armazenamento de créditos eletrônicos correspondentes aos bilhetes adquiridos, deverá estar dentro do processo de Segurança do SIBEM, tendo acesso às chaves de escrita e leitura do cartão e obtendo a assinatura da transação de venda através do HSM (se a transação for realizada *online*, com o equipamento conectado ao Servidor de Recarga do SIBEM) ou SAM (se a transação for *offline*, desconectado do Servidor de Recarga do SIBEM), atendendo os requisitos de autenticidade, integridade e confiabilidade.

A Concessionária consultará o SIBEM, verificando a disponibilidade de poltrona na(s) data(s) / horário(s) solicitados pelo usuário e/ou disponíveis para viagens, ou verificará a reserva(s) existente(s). Estes procedimentos de verificação deverão ser realizados tanto para viagens rodoviárias dentro da mesma área de operação da concessionária quanto para viagens envolvendo áreas de operação de outras concessionárias.

Uma vez identificada a condição que atende a necessidade do usuário, a concessionária iniciará o processo de venda da passagem, obtendo a autenticação do valor da passagem do repositório de créditos eletrônicos e o número sequencial único da transação do HSM-SAM. A transação de venda da passagem deverá possuir uma assinatura eletrônica fornecida pelo HSM-SAM.

Na emissão da passagem, além de conter as informações definidas pela ARTESP, deverá ser impresso um número sequencial único fornecido pelo HSM-SAM, que identificará esta transação.

O usuário poderá efetuar o pagamento da passagem em dinheiro, cartão de débito, cartão de crédito, outros meios aceitos pela Concessionária, ou através de um Cartão Inteligente, contendo créditos eletrônicos (condição válida também para o usuário estudante/professor com direito à gratuidade de 50%).

Na condição de pagamento com Cartão Inteligente, o valor da passagem não será autorizado pelo HSM-SAM, pois a transação financeira já foi autorizada pelo HSM-SAM, quando da carga do Cartão Inteligente.

Este processo de vendas de passagens pode ser realizado também em uma máquina de autoatendimento.

Esta transação deverá ser assinada utilizando módulo SAM e informada à ARTESP.

### **Devolução (Cancelamento) de Passagens**

O usuário, conforme previsto no Anexo III – Regulamento Complementar dos Serviços, poderá efetuar a devolução da passagem para a concessionária, recebendo o valor pago pela mesma de acordo com a Lei. 11.975, de julho de 2009, ou a que vier substituí-la.

### **Troca de Passagens**

Assim como é permitida a devolução de uma passagem, respeitando os limites de prazos estabelecidos, também será possível efetuar a troca da passagem.

Para tal, deverá ser efetuado o cancelamento da passagem atual e então deverá ser emitida uma nova passagem para o usuário, utilizando as transações normais de cancelamento e venda de passagem.

A transação deverá ser assinada utilizando módulo SAM e informada para a ARTESP.



## **Reserva de Passagens**

Todo o processo de controle de reserva de passagens é de responsabilidade e controle exclusivo das Concessionárias.

## **Descontos promocionais em passagens**

Quando a passagem for vendida com descontos promocionais concedidos pelas Concessionárias, deverá ser informado à ARTESP o valor efetivamente praticado.

## **Loja Virtual ou agências de Viagens**

Todo o processo de controle de reserva de passagens pelo canal Loja Virtual ou Agências de Viagens é de responsabilidade e controle exclusivo das Concessionárias.

## **Viagem Escolar - Estudantes e Professores**

Uma vez que o cartão é único, ele poderá ser utilizado para a compra de passagem nas bilheterias, utilizando créditos eletrônicos constantes no mesmo. Alternativamente, o cartão servirá como comprovante da condição de estudante ou professor para aquisição de passagens em dinheiro, cartão de débito, cartão de crédito ou outros meios aceitos pela concessionária.

## **Vendas de Créditos Eletrônicos - Cartão Inteligente**

O usuário, em posse de um Cartão Inteligente, poderá efetuar a aquisição (compra) de créditos eletrônicos correspondentes a um valor em dinheiro, que serão utilizados para pagamento de passagens.

Uma vez que o Cartão Inteligente é único, esta transação de venda de créditos eletrônicos é a mesma já descrita nos requisitos de negócio da modalidade suburbana.

Esta transação deverá ser assinada utilizando módulo SAM e informada à ARTESP.

## **Abertura de Viagem - Motorista**

Uma vez estacionado o ônibus na plataforma de embarque (inicial de partida), o motorista efetuará a abertura de viagem utilizando o seu Cartão Inteligente Motorista, identificando assim o início do embarque.

A partir deste momento, será iniciado o embarque dos passageiros.

Esta transação deverá ser assinada utilizando módulo SAM e informada à ARTESP.

As informações deverão ser enviadas *online* para o CCO da Concessionária e para o SIBEM.

### **Embarque dos Passageiros**

Durante o processo de embarque, os passageiros serão contados, e registrados no validador.

Deverá ser tratada pela Concessionária a contabilização de usuários embarcados em garagens, antes dos terminais rodoviários.

### **Fechamento do Embarque - Motorista**

Uma vez identificado pelo motorista que o processo de embarque foi completado, será apresentado o seu Cartão Inteligente Operacional, efetuando o fechamento do embarque.

A verificação da autenticidade do Cartão Inteligente do condutor e a geração de assinatura para a transação de fechamento de embarque serão realizadas através de módulo SAM. Esta transação deverá ser informada à ARTESP.

As informações deverão ser enviadas *online* para o CCO da Concessionária e para o SIBEM.

### **Paradas Durante a Viagem**

Existirão dois tipos de paradas nas viagens:

- I. **Paradas programadas:** para refeições e locais de desembarque de passageiros constantes no itinerário pré-definido.
- II. **Paradas eventuais:** para embarque/desembarque de passageiros, a critério da Concessionária.

As informações deverão ser enviadas *online* para o CCO da Concessionária e para o SIBEM.

Estas transações serão informadas a ARTESP com as respectivas movimentações de passageiros.

### **Embarque de Passageiros Durante a Viagem**

O embarque durante a viagem poderá ocorrer para passageiros que já possuem a passagem adquirida anteriormente e nas condições e nos locais autorizados pela ARTESP para embarque / desembarque de passageiros.

### **Fiscalização Durante a Viagem**

Para acesso das informações, o fiscal da ARTESP efetuará a sua identificação apresentando o seu Cartão Inteligente, verificando as informações referentes à viagem, bem como a quantidade de passageiros que estão sendo transportados.

A verificação da autenticidade do Cartão Inteligente do fiscal e a geração de assinatura para a transação de fiscalização durante a viagem serão realizadas através de módulo SAM. Esta transação deverá ser informada à ARTESP.

### **Fechamento da Viagem**

Uma vez que a viagem tenha sido completada, o motorista utilizará o seu Cartão Inteligente Operacional para efetuar o fechamento da viagem.

A verificação da autenticidade do Cartão Inteligente do condutor e a geração de assinatura para a transação de fechamento de viagem serão realizadas através de módulo SAM. Esta transação deverá ser informada à ARTESP.

As informações deverão ser enviadas *online* para o CCO da Concessionária e para o SIBEM.

## **3.2. Cadastramento e Manutenção de Parâmetros do Sistema.**

Cada Concessionária deverá manter as tabelas de parametrização no seu sistema SIBEM.

A ARTESP deverá disponibilizar um sistema *online* que implemente um controle de fluxo de processos, onde a concessionária, efetuará o registro da solicitação de inclusão, alteração

ou cancelamento de parâmetros de concessão, tais como veículos, ligações, horários E tarifas.

Após aprovação da solicitação, a Concessionária efetuará a atualização em seu sistema SIBEM, o qual deverá estar sempre atualizado (sincronizado) com as mesmas informações existentes no CCI da ARTESP, quais sejam:

- I. **Veículos:** contendo todas as características funcionais dos veículos, tais como: lotação máxima, área, tipo de veículo, ano de fabricação;
- II. **Ligações:** contendo todas as ligações com seus respectivos atributos, tais como: pontos de parada e respectivas coordenadas GPS, extensões, horários etc.;
- III. **Tarifas:** contendo todos os valores de tarifas correspondentes às ligações e/ou trechos das ligações com tarifas diferenciadas;
- IV. **Equipamentos:** contendo todos os dados dos equipamentos, tais como: tipo, marca, modelo, identificação, fornecedor, veículo instalado (equipamentos de bordo), localização, identificação do SAM.

### 3.3. Monitoramento - Envio de Informações para o CCO

A CONCESSIONÁRIA deverá ter e implantar um Sistema de Monitoramento das Viagens.

Deverá ser um módulo sistêmico de localização dos veículos operacionais de toda a frota da Concessionária em mapas digitais em todo o Estado de São Paulo com informações de rotas de inspeção de tráfego, veículos envolvidos, velocidade, localização, cadastramento de rotas, rotas em aberto, rotas incompletas, pontos de referência, localização do veículo, identificação do condutor, data e hora de início, de retomada e outras. O objetivo é acompanhar via GPS o posicionamento global georreferenciado dos ônibus e veículos operacionais das concessionárias.

Em intervalos de tempo pré-estabelecidos (parametrizado = 2 (dois) minutos), o DGC, via GPRS, deverá enviar as informações para o CCO da concessionária, conseqüentemente para o CCI da ARTESP. Estas informações deverão ser assinadas utilizando o módulo SAM instalado no DGC:

- I. Posicionamento do veículo;

- II. Alarmes;
- III. Abertura de portas;
- IV. Velocidade instantânea.

### 3.4. Segurança

#### 3.4.1. Geração, Armazenamento e Transporte de Chaves Primárias

As chaves primárias constituem a base do sistema de segurança de bilhetagem eletrônica. São utilizadas para derivar as chaves de acesso ao cartão e em todos os algoritmos de criptografia usados nos processos de segurança. Devido ao alto custo computacional dos algoritmos de criptografia assimétricos, são adotados chaves e algoritmos de criptografia simétricos, como o AES.

As chaves devem ser geradas em ambiente seguro, utilizando hardware dedicado (HSM) que garanta a proteção das chaves. Neste processo, as chaves nunca poderão trafegar em aberto, portanto, o processo de geração precisa ser feito por inteiro dentro deste hardware.

Outro requisito importante que deve cumprir o sistema de segurança a ser apresentado pela concessionária é o transporte seguro das chaves do HSM para o SAM, no processo de inicialização deste último. As chaves não podem trafegar abertas (*cleartext*) pela rede, nem serem expostas a nenhuma aplicação, em momento algum.

Para tal é necessário criar uma chave de transporte dentro do HSM, a partir de um procedimento que utilize dois ou mais frases secretas, em poder de pessoas diferentes, para geração da chave de transporte. Utilizando as mesmas frases secretas é possível, na inicialização do SAM, usando o mesmo algoritmo, gerar e armazenar nele a mesma chave de transporte.

#### 3.4.2. Certificação de Créditos

A rede *online* utiliza um Serviço de Recarga Online ou Servidor de Créditos, que atua como “ponte” entre o HSM, no papel de Certificador de Créditos e o terminal de venda. O HSM terá como missão permitir a transferência segura de créditos para o cartão do usuário.

O HSM deverá permitir a execução da seguinte sequência de operações:

- I. Autenticar a solicitação de transferência de créditos: O terminal de venda enviará uma solicitação “carimbada” pelo SAM de PDV, de forma que o HSM possa confiar na origem do pacote. Esta assinatura terá o número de série do SAM como fator de diversificação. O pacote terá ainda contadores de transações do SAM para impedir fraude de repetição de pacotes;
- II. Produzir e assinar criptograma de crédito para recarga e atualização de dados da última recarga do cartão, que tenha como único destino possível o cartão cujos dados foram recebidos na solicitação de crédito anterior;
- III. Gerar e assinar registro de transação de crédito *online*, que deverá ser inserido no banco de dados pelo Servidor de Créditos, para garantir rastreabilidade do processo;
- IV. Calcular chave de escrita para atualização de dados no cartão do usuário.
- V. Enviar pacote de crédito “carimbado” pelo HSM, contendo chave de escrita, que possa ser interpretado apenas pelo solicitante do crédito: o SAM instalado no equipamento que emitiu a solicitação.

Os créditos a serem transferidos para o cartão do usuário também poderão ser procedentes do SAM instalado no equipamento de venda de créditos.

O módulo SAM se abastecerá de créditos através de uma transação *online* que ocorre através do Serviço de Recarga *Online*, que acessa o repositório de créditos do HSM para transferir os mesmos ao SAM e assim possibilitar a sua distribuição off-line.

Nesta modalidade de recarga o SAM executa a mesma sequência de operações descrita anteriormente para o HSM.

### **3.4.3. Fiscalização de Transações de Viagem**

No papel de Fiscalizador de Transações de Viagem originadas nos validadores, o HSM instalado no CCO da Concessionária deve ser capaz de garantir a validação de cada uma das transações de viagem recebidas no Sistema Central de Processamento. Todos os dados da transação recebida, incluída a assinatura, devem ser armazenados no banco de dados, o que permite guardar um registro íntegro que pode ser auditado a qualquer

momento. O hardware e a modelagem da aplicação do HSM devem garantir o tempo de resposta requerido adiante, em função dos altos volumes de transação.

#### **3.4.4. Fiscalização de Transações de Créditos**

No papel de Fiscalizador de Transações de Crédito originadas nos terminais de venda, o HSM do SIBEM deve ser capaz de garantir, com alto desempenho, a validação de cada uma das transações de crédito realizadas nesses terminais. Devido ao alto volume, o HSM deve apresentar os níveis de resposta requeridos adiante para conferencia destas assinaturas.

#### **3.4.5. Certificação de Arquivos**

Todas as listas, arquivos de parâmetros, arquivos de software para o validador, terminal de venda e SAMs deverão ser assinados pelo HSM instalado no CCO da Concessionária, no papel de Certificador de Arquivos.

#### **3.4.6. Geração e armazenamento de crédito**

A geração de crédito deve ser realizada em ambiente controlado e seguro. Os atores principais deste processo são dois elementos de hardware, o Cartão para Geração de Créditos e o Repositório de Crédito, que executam aplicações com acesso a serviços criptográficos localizados em cada dispositivo.

O Cartão para Geração de Créditos deve ser um Cartão Inteligente com contato, compatível com ISO 7816. É um cartão de propriedade exclusiva do responsável pela geração de crédito, que armazena uma senha que será solicitada neste processo.

O Repositório de Crédito deve ser um dispositivo seguro, FIPS 140-2 nível 3, para o qual pode ser utilizado o próprio HSM descrito anteriormente.

Para poder efetuar a geração do crédito deve ser estabelecido um canal de comunicação seguro entre o Cartão e o Repositório, em que ambos participantes se autenticam mutuamente e após esta autenticação, os dados passam a trafegar criptografados. Usando algoritmos de criptografia assimétricos, como o RSA, o crédito gerado em uma determinada origem, o Cartão para Geração de Créditos, pode ser depositado apenas no destino que iniciou a “conversa” com ele, o Repositório de Créditos, pois neste canal uma mensagem cifrada procedente de um deles somente pode ser decifrada pelo outro elemento.

### 3.4.7. Transferência de Crédito do HSM para o SAM de PDV

Com o objetivo de garantir maior disponibilidade nas redes de recarga, devendo manter os mesmos níveis de segurança, o SAM do PDV poderá armazenar créditos eletrônicos, que serão transferidos para o Cartão Inteligente do usuário, quando da realização de cargas.

O SAM deverá manter armazenado um determinado valor de créditos eletrônicos (saldo) armazenado (parametrizado), que será utilizado na carga dos Cartões Inteligentes. Quando este saldo atingir um determinado valor (parametrizado), a aplicação de vendas de créditos, efetua uma solicitação de transferência *online* de créditos eletrônicos da aplicação do HSM para o SAM, utilizando o protocolo ISO-8583.

A condição estabelecida para que a aplicação do HSM realize a transferência dos créditos eletrônicos solicitados é o envio para o HSM, de todas as transações de carga realizadas. A aplicação HSM deverá realizar a conciliação do saldo do SAM com os valores utilizados nas cargas.

A aplicação do HSM deverá gerar um registro que identifica a transação de log de transferência de créditos eletrônicos para o SAM. Esta transação deverá ser assinada. Como mínimo, o log de transferência deve conter os seguintes campos:

- I. NSU (Número sequencial único) da transação;
- II. Identificação do SAM;
- III. Valor da transação de transferência;
- IV. Saldo anterior do SAM (antes da transferência);
- V. Data da transferência;
- VI. Saldo atual do SAM (após a transferência).

Para assegurar a rastreabilidade deste processo, a aplicação executada no servidor deve armazenar no banco de dados, para cada transação, um registro, chamado log de transferência de créditos eletrônicos, contendo informações anteriores, além da própria assinatura do log.



A geração da assinatura do log de transferência é atribuição apenas da aplicação do HSM.

#### **3.4.8. Transferência de Crédito do SAM para Cartões de Usuário**

O processo de recarga de créditos eletrônicos nos cartões dos usuários requer de um elemento de segurança no POS ou PDV, o SAM de PDV, de um Certificador de Créditos (HSM) e de um Repositório de Crédito que garanta a transferência segura do crédito armazenado nele para o cartão do usuário.

Com o objetivo de garantir maior disponibilidade nas redes de recarga, devendo manter os mesmos níveis de segurança, o SAM do PDV poderá armazenar créditos eletrônicos, que serão transferidos para o Cartão Inteligente do usuário, quando da realização de recargas no Cartão Inteligente.

Neste processo, o SAM é responsável pelo fornecimento do valor do crédito eletrônico pela geração das assinaturas dos novos dados do cartão, pois na transação modificam-se tanto o saldo quanto os dados de recarga do cartão. As novas assinaturas e a própria chave de acesso para escrita dos novos dados assinados são fornecidas pelo SAM.

A recarga somente pode ser realizada, se confirmada a integridade do cartão antes da operação, o que deve ser feito pelo SAM.

A aplicação do SAM deve reunir em um registro que identifica a transação, chamado log de recarga, as informações que a caracterizem e deve gerar uma assinatura para esse conjunto de dados. Como mínimo, o log de recarga deve conter os seguintes campos:

- I. Tipo de cartão (comum, estudante, VT);
- II. Tipo de carteira creditada (comum ou especial);
- III. NSU (Número sequencial único) da transação;
- IV. Número do cartão;
- V. Valor da transação;
- VI. Contador de viagens;
- VII. Contador de recarga;

VIII. Data da recarga;

IX. Data da compra do crédito (diferente do campo anterior em caso de créditos pré-pagos);

X. Saldo do cartão.

Para assegurar a rastreabilidade deste processo, a aplicação executada no servidor deve armazenar no banco de dados, para cada transação, um registro, chamado log de recarga, contendo informações anteriores, além da própria assinatura do log.

A transferência de créditos do SAM para o cartão do usuário segue a mesma sequência de operações descrita anteriormente.

### 3.5. Níveis de Serviço

O projeto, a implantação, a operação e a manutenção do SIBEM e do CCO deverão ser desenvolvidos de forma que sejam atendidos os níveis de desempenho descritos no Anexo IV – Índices de Desempenho do Serviço.

## 4. Migração da Situação Atual para o Modelo ARTESP

A migração deve ser entendida em dois contextos: concessionárias que não possuam recursos sistêmicos e embarcados pré-existentes ou cujos recursos existentes, não sejam aderentes ao Modelo ARTESP; e concessionárias cujos recursos sistêmicos e embarcados pré-existentes sejam aderentes ao Modelo ARTESP.

O processo de migração deve ocorrer no prazo máximo de 26 meses após o início de operação.

Este procedimento é composto dos seguintes passos:

I. **Homologação de fornecedores:** alguns equipamentos que farão parte do sistema deverão passar por um procedimento de homologação. O processo de homologação será definido em portaria específica;

II. **Instalação dos equipamentos ou adequação do parque:** os equipamentos deverão ser instalados ou deverão sofrer as adequações necessárias para o início da operação com o novo sistema. Na hipótese mais simples, os equipamentos sofrerão alterações de firmware e será inserido em seu interior um SAM da ARTESP para controle das operações, caso contrário, onde não houver condições técnicas de usar o parque atual ou não existir uma instalação prévia, devem ser instalados equipamentos homologados com o SAM da ARTESP instalado;

III. **Cartões:** serão considerados cartões compatíveis com o sistema aqueles que possuírem as características exigidas neste documento. Neste caso, estes cartões serão migrados através de processo realizado junto ao validador e máquinas de recarga, que “reformatarão” os cartões para o novo modelo. Após o início da operação, apenas serão aceitos cartões que sejam compatíveis e os demais cartões serão rejeitados;

IV. **Sistemas de Venda e Garagem:** todos devem ser revistos e devem seguir o especificado no item segurança deste Edital.

O processo de migração, além dos aspectos expostos acima, se caracteriza pela definição e implementação do SIBEM e CCO, nos seguintes prazos:

- I. Apresentação do projeto à ARTESP em até 12 (doze) meses após a data de início de operação;
- II. Aprovação e homologação da ARTESP em até 60 (sessenta) dias após a apresentação do projeto;
- III. Implantação em até 12 (meses) a partir da aprovação pela ARTESP.

## 5. Itens de Segurança

### 5.1. HSM - Hardware Security Module

É um dispositivo de hardware que permite o armazenamento seguro das chaves primárias e a execução de algoritmos de hashing, criptografia simétrica e assimétrica com alto desempenho.

A concessionária deverá utilizar um sistema de segurança baseado no uso de HSMs, detalhando fabricante, algoritmos de criptografias suportados, índices de desempenho e facilidades de escalabilidade.

O HSM deverá ser um equipamento tipo appliance, com interface para conexão em rede local. Deverá também estar capacitado para:

- I. Gerar de forma segura as chaves primárias do sistema de segurança (um ou mais lotes caso necessário).
- II. Proteger as chaves primárias geradas. O HSM precisa cumprir com rigorosas exigências de segurança para garantir que as chaves fiquem protegidas sob “lacre” inviolável, jamais possam ser acessadas por nenhum tipo de invasão nem exportadas em aberto. Em caso de tentativa de invasão, o HSM deverá destruir as chaves e parâmetros críticos de segurança;
- III. Gerar e verificar assinaturas de logs de transações usando as chaves primárias geradas;
- IV. Gerar e verificar assinaturas de arquivos usando uma das chaves primárias geradas. Os arquivos de parâmetros, de listas de restrição e de software deverão ser assinados pelo HSM;
- V. Hospedar e proteger a aplicação criptográfica que contém as funções de segurança do sistema. Deve garantir que não seja possível realizar alterações indevidas na aplicação, debug ou decompilação para engenharia reversa e que somente aplicações devidamente autorizadas possam ser colocadas ou atualizadas no interior do HSM;
- VI. Realizar backup das chaves primárias e recuperar tais chaves apenas em hardware do mesmo tipo, sem exposição das chaves em aberto em qualquer canal de comunicação ou para qualquer aplicação fora do HSM;
- VII. Executar funções de criptografia simétricas e assimétricas em hardware, com altíssimo desempenho;
- VIII. Gerar chaves de acesso diversificadas para os cartões do usuário usando as chaves primárias geradas;

- IX. Autenticar qualquer aplicação que deseje utilizar os serviços do HSM mediante mecanismos seguros de autenticação mútua;
- X. Servir como repositório de crédito;
- XI. Permitir hospedar várias aplicações criptográficas, com chaves e repositórios de créditos independentes, garantindo a não interferência entre aplicações.

Para garantir a proteção das chaves e parâmetros críticos de segurança, o HSM a ser oferecido pela concessionária deve ser certificado pela norma FIPS 140-2 nível 3. O certificado FIPS (Federal Information Processing Standards) é oferecido pelo National Institute of Standards and Technology (NIST) e especifica as exigências de segurança que devem ser preenchidas pelas soluções de criptografia. O certificado FIPS 140-2 nível 3 garante que o hardware está protegido contra:

- I. Violação física do equipamento;
- II. Desligamento da rede de alimentação por tempos acima do normal;
- III. Acessos de usuários não autorizados;
- IV. Tráfego de chaves.

Diante de qualquer invasão o HSM deve destruir automaticamente todos os parâmetros críticos de segurança e as chaves de criptografia armazenadas nele. A tecnologia que será adotada para o HSM deve permitir uma fácil e rápida escalabilidade, que permita, em um prazo máximo de 48h, aumentar a capacidade de processamento do HSM, executando nesse período os seguintes processos:

- I. Instalação e configuração do HSM;
- II. Replicação segura de chaves primárias;
- III. Instalação e configuração de servidores criptográficos para acesso e utilização da nova capacidade de processamento.

## 5.2. Geração, armazenamento e transporte de chaves primárias

### 5.2.1. SAM

O Módulo de Segurança de Acesso - SAM (Secure Access Module) é um dispositivo de hardware utilizado para proteger o acesso a Cartão Inteligente, disponibilizar algoritmos de criptografia e regular o comportamento das aplicações que manipulam esses cartões.

O SAM deve ser compatível com ISO-7816 e ter formato ID-000. Deve estar protegido contra acessos indevidos, homologado pela norma FIPS 140-2 nível 3. Essa proteção faz se necessária, pois o SAM, em um modelo de segurança com criptografia simétrica, como o que será utilizado no Sistema de Bilhetagem, armazena as chaves primárias do sistema e os algoritmos que permitem executar operações criptográficas utilizando essas chaves.

O SAM deve permitir, em equipamentos como validadores, DGCs e dispositivos de venda de créditos:

- I. Obter chaves diversificadas para cada cartão e cada tipo de dados armazenado nele, fornecendo acesso apenas aos dados que cada aplicação manipula, dependendo do perfil definido no próprio SAM, utilizando como fator de diversificação o número de série do cartão;
- II. Verificar assinaturas eletrônicas para cada tipo de dado;
- III. Gerar novas assinaturas para novos dados do cartão;
- IV. Verificar assinaturas de pacotes que contem parâmetros, listas de restrição e novas versões de software;
- V. Assinar registros contendo informações de transações;
- VI. Assinar arquivos que devem ser enviados ao sistema central;
- VII. Atualizar-se automaticamente com novas versões de software recebidas.

É importante também ressaltar que o SAM a ser adotado deve permitir armazenar separadamente várias aplicações, cada uma com seu conjunto de chaves, para garantir interoperabilidade segura entre diferentes gestores do sistema de transporte. O SAM deverá permitir a separação física das chaves e aplicações de cada empresa e a atribuição

individualizada de permissões para obtenção de chaves de acesso aos cartões emitidos pelas outras empresas, conforme critérios utilizados na criação do SAM.

### **Tipos de SAMs**

Cada tipo de dado do cartão é protegido com chaves dedicadas (diferentes uma da outra). Isto permite conceder permissões de acesso aos dados do cartão conforme o perfil da aplicação que os utiliza. Este conceito permite classificar os SAMs conforme o tipo de aplicação que os utilizará:

- I. SAM de Validador: permite ler todo o conteúdo do cartão, conferir assinaturas do cartão, alterar os dados da última transação e o saldo, assinando os novos dados derivados desta alteração.
- II. SAM de PDV: permite ler todo o conteúdo do cartão, conferir assinaturas do cartão, alterar os dados da última recarga e o saldo, assinando os novos dados derivados desta alteração;
- III. SAM de DGC: permite apenas assinar registros de eventos operacionais que serão enviados ao Sistema de Monitoramento de Frota;
- IV. SAM de Emissão: Permite inicializar cartões de usuário, gravando nele dados assinados e chaves de acesso.

### **5.2.2. Máquina de Estados**

O módulo SAM deve ser capaz de controlar o fluxo das aplicações instaladas nos equipamentos do Sistema de Bilhetagem. Para tal o SAM utiliza uma máquina de estados, que força as aplicações a executar regras de negócio específicas, em determinada ordem, e define as transições de estado que garantam um fluxo seguro de operações.

Cada tipo de SAM tem sua própria máquina de estado, para executar as operações próprias em uma sequência segura. Cada operação da máquina de estado no SAM deverá gerar um código hash de estado derivado dos dados utilizados na operação, que servirá de entrada na próxima fase do processo.

Segue uma típica ordem de execução que deverá ser utilizada como guia para implementação da máquina de estados:

- I. Fornecer chaves de acesso de leitura ao cartão, com base no número de série;
- II. Verificar assinatura eletrônica de todos os dados do cartão. Se for detectado qualquer problema de integridade, retornar ao estado inicial da máquina de estados;
- III. Gerar assinaturas eletrônicas para os novos dados do cartão, utilizando como referência para validação os dados atuais e os novos dados. Esta operação dependerá do tipo de SAM, que definirá os níveis de acesso aos diferentes tipos de dados do cartão;
- IV. Gerar assinatura de registro da transação, conforme o tipo de operação.

### 5.2.3. Requisitos dos Cartões

Para garantir a migração para o novo Sistema de Bilhetagem é necessário que o cartão, além de possuir as especificações técnicas mencionadas no item 7 deste documento, tenha ao menos espaço suficiente para armazenar os seguintes dados:

- I. Número sequencial do cartão;
- II. Data da emissão ou migração do cartão;
- III. Tipo do cartão;
- IV. Validade do cartão;
- V. Tipo de usuário e identificação de usuário para o caso de cartões personalizados;
- VI. Restrições de uso, por período e por faixa horária;
- VII. Contadores de uso para verificação das restrições anteriores;
- VIII. Contadores de integração;
- IX. Dados referentes à última transação de crédito do cartão: código do terminal de venda, do SAM, da rede credenciada, do crédito realizado, data;
- X. Saldo financeiro disponível para consumo;



XI. Dados referentes à última transação de débito do cartão: código do validador, do SAM, da empresa transportadora, da ligação, do veículo, tarifa, latitude e longitude, data e hora;

XII. Assinaturas eletrônicas.

Em caso de sistemas em operação, o cartão em uso deve ter configurações de acesso que possibilitem:

- I. Ler dados da aplicação atual;
- II. Gravar dados do novo sistema em setores disponíveis;
- III. Modificar chaves e perfil de acesso aos novos dados;

## **6. Eletrônica Embarcada**

### **6.1. Itens Comuns ao Suburbano e Rodoviário**

#### **6.1.1. Validadores**

O validador tem como função principal verificar se o cartão apresentado pelo usuário o autoriza a realizar a viagem. Para tal, o validador deve checar a autenticidade do cartão através do módulo SAM e posteriormente efetuar a transação de débito no cartão do usuário.

O resultado da transação deverá ser informado através do display do validador, de sinais luminosos e de sinais sonoros diferenciados.

Para os cartões viagem unitária suburbana (usuários eventuais), no validador de entrada, através da apresentação do cartão (coordenada GPS do ponto de origem) e da informação alimentada pelo condutor ou cobrador, do ponto de destino, através do TD - terminal de dados, o validador de entrada efetuará o cálculo do valor da tarifa, informando ao condutor o valor a ser pago pelo usuário.

O validador poderá ser usado, também, na modalidade rodoviária para registrar o bilhete de passagem, contabilizando o embarque do passageiro no terminal.

O validador também deve permitir o controle do serviço do operador do veículo, através de operações como abertura e fechamento de serviço e transação de meia viagem. Na modalidade suburbana existirá um segundo validador, com função de saída e recolhimento de cartões para o caso de usuários eventuais.

### Requisitos dos Equipamentos

Para poder operar no Sistema de Bilhetagem os validadores devem possuir os seguintes requisitos mínimos:

- I. Leitor de cartão eletrônico sem contato, compatível com ISO 14.443 A e B, distância máxima de operação de 100 mm;
- II. Pelo menos um soquete disponível ID-000 para o chip SAM, e interface de comunicação em estado operacional com este dispositivo;
- III. Uma porta de comunicação RS-485 disponível para interface com dispositivo de Geoposicionamento e comunicação;
- IV. Microprocessador com função de boot loader para atualização de software;
- V. Memória volátil para execução de programas;
- VI. Memória não volátil suficiente para armazenamento de parâmetros e logs de transações e operações realizadas;
- VII. Display de caracteres de duas ligações para interface com os usuários e o operador;
- VIII. Sinal luminoso verde para indicar transação de usuário bem-sucedida;
- IX. Sinal luminoso vermelho para indicar algum erro ou restrição para uso do cartão do usuário;
- X. Sinal sonoro (*buzzer*) para indicar resultado da transação de forma diferenciada;
- XI. Mecanismo por radiofrequência para coleta de arquivos e atualização de parâmetros e software;

XII. Mecanismo de leitura, coleta e guarda de cartões no validador de saída da modalidade suburbana;

XIII. Interface de manutenção USB, RS-232 ou Ethernet;

XIV. Tempo médio de processamento de débitos do cartão no validador inferior a 400 milissegundos, limitada a 800 milissegundos em 0,001% das passagens.

### **Interface com Outros Sistemas**

O validador deve estar preparado para receber vários tipos de arquivos de dados do SIBEM: parâmetros de listas de restrição, software do validador e do SAM e, inclusive, arquivos contendo novas chaves do sistema, para gravação no SAM. Os arquivos recebidos virão assinados eletronicamente e o validador, através do SAM, será capaz de validá-los e interpretá-los adequadamente.

Do validador deverão ser enviados ao CCO os arquivos de transações de usuários e de serviço, assinados pelo SAM de validador. Um resumo das transações realizadas, agrupadas por tipo de cartão, deverá ser assinado e enviado do validador ao equipamento de geoposicionamento e comunicação, de tempos em tempos, para que este o encaminhe ao CCO.

O validador deverá interagir com o equipamento de geoposicionamento e comunicação (descrito mais adiante) para obter um pacote de dados de localização geográfica assinado pelo SAM instalado neste equipamento, toda vez que seja necessário produzir informações georreferenciadas no validador.

O validador e o equipamento de geoposicionamento e comunicação se autenticarão mutuamente utilizando processos de segurança coordenados pelos SAMs instalados nesses equipamentos.

### **Requisitos de Software**

Os fabricantes dos validadores, tanto os que já estão em operação quanto aqueles que venham a ser credenciados futuramente pela ARTESP, deverão passar por um processo de homologação. Este deverá capacitar o validador para executar as seguintes operações:

I. Checar a presença do módulo SAM e impedir qualquer operação caso esteja ausente;

- II. Executar os comandos da máquina de estados do SAM de validador na ordem estabelecida;
- III. Receber e se atualizar com novas versões de software;
- IV. Mediar a atualização do software do SAM;
- V. Permitir a atualização de chaves primárias do SAM;
- VI. Interagir com o módulo de Geoposicionamento e comunicação para produzir dados georreferenciados e enviar resumo de dados de bilhetagem;
- VII. Viabilizar a migração dos cartões do sistema atual para o novo, quando aplicável;
- VIII. Integrar-se a outros equipamentos mediante autenticação mútua, com suporte do SAM;
- IX. Tempo máximo da transação com cartão de usuário inferior a 800 ms, envolvendo acesso ao cartão e as funções do SAM.

### **6.1.2. Terminal de Dados**

A entrada de dados será realizada através de um teclado, conectado ao validador, instalado próximo ao motorista.

### **Requisitos do Equipamento**

O terminal de dados deve possuir os seguintes requisitos mínimos:

- I. Display
- II. Sinal luminoso verde para indicar transação bem-sucedida;
- III. Sinal luminoso vermelho para indicar erro;
- IV. Sinal sonoro (*buzzer*) para indicar resultado da transação de forma diferenciada;
- V. Comunicação em RS-232;
- VI. Possuir uma porta de comunicação serial auxiliar;

VII. Interface de manutenção USB, RS-232 ou Ethernet.

### **Interface com Outros Sistemas**

O terminal de dados deve estar preparado para receber do SIBEM arquivos de configuração e de software do próprio terminal de dados. Os arquivos recebidos virão assinados eletronicamente e o terminal de dados, através do SAM instalado no validador, deverá ser capaz de validá-los e interpretá-los adequadamente.

### **Requisitos de Software**

Os fabricantes dos terminais de dados, tanto os que já estão em operação quanto aqueles que venham a ser credenciados futuramente pela ARTESP, deverão passar por um processo de homologação. Este deverá capacitar o terminal de dados para executar as seguintes operações:

- I. Checar a comunicação com o validador;
- II. Receber e se atualizar com novas versões de parâmetros e software.

#### **6.1.3. Dispositivo de Geoposicionamento e Comunicação - DGC**

O dispositivo de geoposicionamento e comunicação (DGC) permite a obtenção de coordenadas geográficas do veículo para geração de informações georreferenciadas.

Este dispositivo estará dotado de um módulo SAM. O software que controla o funcionamento deste dispositivo deverá interagir com o SAM para reconhecer a autenticidade de outros dispositivos conectados a ele e para gerar pacotes de informação assinados, que certifiquem a origem e qualidade destas informações.

O DGC permite o envio de informações de bilhetagem, procedentes do validador, e de passageiros que embarcaram e desembarcaram procedentes do contador de passageiros.

### **Requisitos do Equipamento**

Para poder operar no Sistema de Bilhetagem os DGCs devem possuir os seguintes requisitos mínimos:

- I. Pelo menos um soquete disponível ID-000 para o chip SAM, e interface de comunicação em estado operacional com este dispositivo;
- II. Uma porta de comunicação RS-485, ou 2 portas RS-232, disponível/disponíveis para interface com validador e com contador de passageiros;
- III. Microprocessador, podendo atuar em modo *polling* ou requisição, com função de *boot loader* para atualização de software;
- IV. Memória volátil para execução de programas;
- V. Memória não volátil suficiente para armazenamento de parâmetros e logs de transações e operações realizadas;
- VI. Modem GSM quadriband com capacidade para duas operadoras de celular;
- VII. Controlador GPS e antena embarcada interna;
- VIII. Compatível com GPS;
- IX. Mínimo de 32 canais de aquisição;
- X. Supervisão de antena integrada;
- XI. Bateria backup;
- XII. Protocolo NMEA 2.3 ou superior;
- XIII. Interface de manutenção USB, RS-232 ou Ethernet (Webserver).

### **Interface com Outros Sistemas**

O DGC deve estar preparado para receber do SIBEM arquivos de configuração, de software do equipamento, software do SAM e, inclusive, arquivos contendo novas chaves do sistema, para gravação no SAM. Os arquivos recebidos virão assinados eletronicamente e o DGC, através do SAM, será capaz de validá-los e interpretá-los adequadamente.

Do DGC deverão ser enviados ao CCO mensagens de posicionamento, assinadas pelo SAM.

O DGC também responde pelo envio ao CCO de resumos de transações procedentes do validador, bem como de informações de contagens apuradas pelo contador de passageiros.

O DGC deverá enviar coordenadas de GPS aos dispositivos instalados nos ônibus que precisam desta informação para geração de eventos georreferenciados relacionados à sua operação, como o validador e o contador de passageiros.

### **Requisitos de Software**

O software do DGC terá os seguintes requisitos:

- I. Checar a presença do módulo SAM e impedir qualquer operação caso esteja ausente;
- II. Executar os comandos da máquina de estados do SAM de DGC na ordem estabelecida;
- III. Receber e se atualizar com novas versões de software;
- IV. Mediar a atualização do software do SAM;
- V. Permitir a atualização de chaves primárias do SAM;
- VI. Interagir com o validador e o contador de passageiros usando protocolo de comunicação a ser definido;
- VII. Integrar-se a outros equipamentos mediante autenticação mútua, com suporte do SAM;

## **6.2. Itens Exclusivos Suburbano**

### **6.2.1. Validador na Saída do Ônibus**

Nos ônibus da modalidade suburbana, devido ao fato das tarifas serem seccionadas por trecho, existirá um segundo validador na saída do ônibus, que permitirá realizar a cobrança conforme o trecho percorrido pelo usuário, comparando o ponto de origem, gravado pelo validador de entrada, com o ponto de destino, detectado pelo validador de saída. O processo funciona da seguinte forma:

- I. O usuário apresenta o cartão no validador à entrada do ônibus;

II. O validador registra no cartão o ponto de origem correspondente à coordenada levantada pelo GPS, com auxílio do DGC;

III. Ao descer do ônibus o usuário apresenta o cartão no validador à saída, que efetua o cálculo da tarifa a ser debitada no cartão do usuário, debita do cartão e libera em seguida a catraca.

Para os cartões viagem unitária, pertencentes a usuários eventuais, o validador efetuará a validação da tarifa cobrada, correspondente ao ponto de origem e o ponto de destino real, caso a tarifa seja maior, a catraca de saída não será liberada e será solicitado o pagamento do complemento ao usuário.

Este validador deve cumprir com as mesmas especificações e requisitos de software apresentados anteriormente, incluindo:

- I. Dispositivo para recolhimento de Cartão Inteligente (cartões viagem unitária);
- II. Interface com a catraca eletrônica.

#### **6.2.2. Catraca Eletrônica**

A catraca eletrônica, destinada à instalação embarcada para o controle de saída em ônibus suburbano, através da liberação feita pelo validador eletrônico de Cartões Inteligentes, deve possuir:

- I. Grande resistência a vibrações e impactos constantes;
- II. Relógio contador mecânico de cinco dígitos acionado por engrenagem;
- III. Solenóide de acionamento de alta durabilidade (PL100%);
- IV. Sensores de giro indutivo;
- V. Trava comutadora, para liberar mecanicamente a saída em situações de falha de liberação do validador e situações de emergência.



### 6.3. Item exclusivo do Rodoviário

#### 6.3.1. Contador de Passageiros

O contador de passageiros é um dispositivo que será instalado nos ônibus para fiscalizar a entrada e saída de passageiros. O Contador de Passageiros deverá estar integrado a toda infraestrutura descrita neste documento referente à Bilhetagem, Monitoramento e Segurança, e toda a informação gerada a partir do dispositivo deverá, também estar disponível à ARTESP.

Este equipamento também deverá ser dotado de um módulo SAM. O software que controla o funcionamento deste dispositivo deverá interagir com o SAM para reconhecer a autenticidade de outros dispositivos conectados a ele e para gerar pacotes de informação assinados, que certifiquem a origem e qualidade destas informações.

#### Requisitos do Equipamento

Para poder operar dentro do Sistema de Bilhetagem, os contadores de passageiros devem possuir os seguintes requisitos mínimos:

- I. Precisão de no mínimo 92%;
- II. Módulo de captura e processamento digital, dotado de algoritmo de especializado em controle e contagem de fluxo de passageiros;
- III. Sensor de abertura e fechamento de portas;
- IV. Uma porta de comunicação RS-485 disponível para interface com DGC;
- V. Microprocessador com função de boot loader para atualização de software;
- VI. Memória volátil para execução de programas;
- VII. Memória não volátil suficiente para armazenamento de parâmetros e logs de transações e operações realizadas;
- VIII. Interface de manutenção USB, RS-232 ou Ethernet;
- IX. IP 50.

## Interface com Outros Sistemas

O contador de passageiros deve estar preparado para receber do SIBEM arquivos de configuração e de software do próprio equipamento. Os arquivos recebidos virão assinados eletronicamente e o contador de passageiros, comunicando-se com o SAM de DGC, será capaz de validá-los e interpretá-los adequadamente.

Do contador de passageiros deverão ser enviados ao CCO os registros de contagens realizadas, assinados pelo SAM de DGC.

Para geração de eventos de contagens georreferenciados, o contador de passageiros deverá obter do DGC as coordenadas de GPS.

## Requisitos de Software

O software do contador de passageiros deve ser capaz de:

- I. Identificar e contabilizar passageiros, permitindo contagem bidirecional e registrando em memória os eventos de contagem georreferenciados e assinados pelo SAM de DGC;
- II. Alta performance para execução dos processos de aquisição, identificação do alvo e processamento de imagens;
- III. Reconhecimento individual de passageiros mesmo quando trafegando em grupos na região de detecção;
- IV. Checar a comunicação com o módulo SAM do DGC e impedir qualquer operação caso houver falha na comunicação;
- V. Executar os comandos respeitando a sequência da máquina de estados do SAM de DGC;
- VI. Receber e se atualizar com novas versões de software;
- VII. Mediar a atualização do software do SAM;
- VIII. Permitir a atualização de chaves primárias do SAM;
- IX. Interagir com o DGC usando protocolo de comunicação a ser definido.

## 7. Cartões Inteligentes e Equipamentos de Venda

### 7.1. Cartões Inteligentes

A tecnologia adotada para o Sistema de Bilhetagem compreende a utilização de cartões sem contato (Cartão Inteligente *contactless*) com circuito integrado. Para os sistemas que já estão em operação é requisito indispensável a adoção desta tecnologia, para garantir a implantação do Sistema de Bilhetagem objeto desta licitação. As características básicas serão definidas em portaria específica da ARTESP.

#### 7.1.1. Requisitos de Segurança

O sistema de segurança a ser adotado no SIBEM, no que se refere aos cartões de padrão aberto, deverá possuir as seguintes características:

- I. Utilizar chaves de acesso diversificadas pelo número serial do cartão, que é único conforme especificação do fabricante do chip. Esta medida de segurança impede a clonagem de cartões no caso da quebra das chaves de algum cartão de usuário;
- II. Separar em arquivos diferentes tipos de dados diferentes (emissão, restrições de uso, viagens, recargas, saldos), para permitir a concessão de permissões de acesso diferenciadas;
- III. Para cada tipo de perfil de usuário deve-se utilizar chaves dedicadas (diferentes umas das outras). Isto permite conceder permissões de acesso e interações aos dados do cartão conforme o perfil da aplicação que os utiliza. Exemplo: o validador utiliza um SAM que concede acesso para alterar o saldo e viagens; o terminal de venda utiliza um SAM que garante acesso de escrita para arquivos de recarga e saldo; o terminal de consulta utiliza um SAM que garante acesso de leitura do saldo e das últimas viagens realizadas;
- IV. Utilizar assinaturas eletrônicas como certificados de integridade dos dados. Isto garante que os dados continuem protegidos, mesmo na hipótese de quebra de chaves. As assinaturas eletrônicas também devem ser diversificadas em função do número serial do

cartão. Isto permite adotar estratégias de tipificação de assinaturas, de acordo com o tipo de dados a ser assinado;

V. Utilizar condições de acesso que permitam trocas de chaves e das próprias condições de acesso;

VI. Usar contadores de decremento que impeçam a fraude de espelhamento (cópia de imagem *mirror* do cartão previamente armazenada);

VII. Chip resistente a ataques de DPA (Análise diferencial do consumo de energia) e DFA (Análise diferencial de falhas), que ofereça AES-MAC para garantir a integridade da sequência de comandos de AES-ENC para garantir a confidencialidade na transmissão de dados;

VIII. Compatibilidade com a criptografia dos atuais sistemas para garantir uma migração suave;

IX. O envio de dados cifrados deve ser feito alterando-se a chave de sessão a cada envio de comando, evitando a utilização da chave para próximos comandos na possibilidade da chave ser quebrada.

As chaves e algoritmos que permitem gerar as assinaturas eletrônicas não devem fazer parte das aplicações do sistema, devem estar protegidos nos SAMs, apresentados anteriormente neste documento.

### **7.1.2. Utilização do Cartão Eletrônico**

Ao utilizar seu cartão, o usuário receberá informações do validador através de três formas: um anunciador sonoro, um display gráfico e um sinalizador com duas posições luminosas nas cores verde e vermelha.

O sinalizador visual, no caso do validador do sistema suburbano, orienta o usuário sobre o resultado do processamento de seu cartão:

I. A luz verde autoriza o embarque ou desembarque do usuário;

II. A luz vermelha no validador de entrada indica problema no cartão (exemplo: crédito negativo, cartão cancelado, etc.) e não valida o processo de registro de abertura de viagem;

III. A luz vermelha no validador de saída indica problema no cartão ou, no caso de usuário eventual crédito insuficiente, e mantém a catraca travada.

O display fornece mensagens aos usuários sobre o estado atual do seu cartão (valor debitado, saldo remanescente, data de validade, etc.), a razão da recusa ou do problema com o cartão e mensagens para o pessoal de manutenção (tipo de falha, erros de transmissão, etc.).

O validador emite, associado à sinalização visual acima descrita, um sinal sonoro, nas seguintes situações:

- I. Cartão não validado pela regra de negócio;
- II. Cartões Gratuito ou Escolar validado com sucesso;
- III. Cartões comum ou VT validado com sucesso.

Ao ser aproximado do validador, o cartão do usuário pode apresentar as seguintes condições:

I. **Cartão Válido:** quando é aproximado da zona de leitura do validador o cartão é processado e o usuário é informado, pelo display, sobre o valor debitado e o saldo (ou tempo de validade para gratuidades) remanescente. Debitado o valor correspondente, o usuário afasta o cartão da zona de leitura e acende-se a luz verde, indicando que a catraca está liberada. A leitora do validador estará apta a processar outro cartão somente após o giro da catraca ter sido completado.

II. **Cartão não Válido, sem Crédito, com Créditos Insuficientes:** quando é aproximado da zona de leitura, o cartão é processado, acende-se a luz vermelha, soa um sinal sonoro, e o usuário é informado pelo display do motivo da recusa do cartão, permanecendo a catraca travada.

III. **Cartão Incluso na Lista de Cartões Cancelados:** quando é aproximado da zona de leitura, o cartão é processado, acende-se a luz vermelha, soa um sinal sonoro, e o usuário é informado pelo display do motivo da recusa do cartão, permanecendo a catraca travada. No

cartão é gravado um código de cancelamento, que impede a utilização daquele cartão novamente.

## 7.2. Terminal de Venda

O terminal de venda é um dispositivo que permite a recarga de créditos através de transações *online*, tanto de créditos pré-pagos (recarga por lista no servidor) como de créditos pagos no ato da recarga.

O terminal deverá estar preparado também para realizar recargas off-line, sem conexão com o Servidor de Recarga Online. Neste tipo de recarga o terminal deverá interagir com o SAM de PDV, que age como repositório e certificador de créditos na transação.

O SAM terá um estoque de créditos eletrônicos. Esse estoque deverá ser monitorado pelo terminal de venda e, caso necessário, deverá ser efetuada uma transação *online* de abastecimento de créditos, isto é, uma transferência do Repositório de Crédito (HSM) para o SAM de PDV.

### Requisitos do equipamento

O terminal de venda fixo deve possuir os seguintes requisitos mínimos:

- I. Leitor de cartão eletrônico sem contato, compatível com ISO 14.443 A e B, distância máxima de operação de 100 mm;
- II. Pelo menos um soquete disponível ID-000 para o chip SAM, e interface de comunicação em estado operacional com este dispositivo;
- III. Microprocessador com função de *boot loader* para atualização de software;
- IV. Memória volátil para execução de programas;
- V. Memória não volátil suficiente para armazenamento de parâmetros e logs de transações e operações realizadas;
- VI. Display de caracteres de duas ligações para interface com os usuários e o bilheteiro;
- VII. Impressora térmica para emissão de comprovantes de venda;

VIII. Interface de comunicação com o Sistema Central: Ethernet ou GSM/GPRS.

### **Interface com outros Sistemas**

Para realizar as operações *online* de recarga de cartões de usuário e de transferência de crédito para o SAM de PDV, o terminal de venda deve se conectar a uma rede *online*. Do lado do servidor, as recargas serão autorizadas através de um serviço TCP, o Servidor de Recarga Online, que implementa um protocolo baseado na norma ISO-8583.

A rede de distribuição de créditos deverá fornecer um Serviço Concentrador, que será responsável pelo gerenciamento dos terminais de venda e agirá como intermediário entre esses terminais e o Servidor de Recarga Online.

Cada rede de distribuição, ou seja, cada Serviço Concentrador da Rede terá um número limitado de conexões com o Serviço de Recarga *Online* da Concessionária. O Concentrador deverá implementar o protocolo de mensagens a ser fornecido pela ARTESP.

### **Requisitos de Software**

Para se credenciar junto a ARTESP, as redes de distribuição de crédito devem observar alguns requisitos relativos à implementação do software que controla os terminais de venda. Estes requisitos são:

- I. Checar a presença do módulo SAM e impedir qualquer operação caso esteja ausente;
- II. Executar os comandos da máquina de estados do SAM de PDV na ordem estabelecida;
- III. Receber e se atualizar com novas versões de software;
- IV. Mediar a atualização do software do SAM;
- V. Permitir a atualização de chaves primárias do SAM;
- VI. Viabilizar a migração dos cartões do sistema atual para o novo, quando aplicável;
- VII. Assinar as operações realizadas através do módulo SAM.

### 7.3. Equipamento de Autoatendimento

Estes dispositivos de autoatendimento serão instalados pela concessionária em locais de grande circulação de usuários, com o intuito de proporcionar a venda auto assistida de recargas de cartões de usuário. Para tal o usuário deverá inserir na máquina as cédulas e moedas que desejar, para efetuar a recarga do valor pago no seu cartão.

Esse equipamento também deverá fornecer informações sobre viagens, sistema de bilhetagem, forma e vantagens do uso do cartão deste sistema, mensagens institucionais e educativas, entre outras informações.

O equipamento de autoatendimento deve permitir a recarga de créditos através de transações *online*, quando estiver conectado ao Servidor de Recarga *online* e *offline*, quando não estiver.

Na transação *offline* o equipamento de autoatendimento deverá interagir com o SAM de PDV instalado nele, que age como repositório e certificador de créditos na transação.

O SAM de PDV terá um estoque de créditos eletrônicos. Esse estoque deverá ser monitorado pelo equipamento de autoatendimento e, caso necessário, deverá ser efetuada uma transação *online* de abastecimento de créditos, isto é, uma transferência do Repositório de Crédito (HSM) para o SAM.

#### **Requisitos do Equipamento**

As máquinas de autoatendimento deverão atender os seguintes requisitos de funcionamento e arquitetura:

- I. Portas frontais independentes para acesso a rolo de impressora e cofre de cédulas e moedas;
- II. Antivandalismo;
- III. Arquitetura da eletrônica baseada em computador industrial;
- IV. Monitor *touch screen*;
- V. Dispositivo de Áudio polifônico com capacidade de executar locuções;



- VI. Impressora térmica, com sistema de corte automático;
- VII. Fácil mecanismo de troca de papel;
- VIII. Introdução de cédulas e moedas pela parte frontal;
- IX. Aceitar todas as cédulas e moedas vigentes no Brasil na data de lançamento do edital. Aceitação de futuras cédulas e moedas mediante reconfiguração;
- X. Taxa de aceitação de cédulas e moedas superior a 95%;
- XI. Taxa de rejeição de moedas fraudulentas superior a 98%;
- XII. Cofre de arrecadação de fácil retirada, com mecanismo de autofechamento automático e sensores;
- XIII. Leitor de cartão eletrônico sem contato, compatível com ISO 14.443 A e B, distância máxima de operação de 100 mm;
- XIV. Pelo menos um soquete disponível ID-000 para o chip SAM, e interface de comunicação em estado operacional com este dispositivo;
- XV. IP 53;
- XVI. Mecanismos de monitoramento remota;
- XVII. Conectividade Ethernet e GPRS;
- XVIII. Modem GSM *quadriband* com capacidade para duas operadoras de celular.

### **Interface com outros Sistemas**

Para realizar as operações *online* de recarga de cartões de usuário e de transferência de crédito para o SAM de PDV, o equipamento de autoatendimento deve se conectar a uma rede *online*. Do lado do servidor, as recargas serão autorizadas através de um serviço TCP, o Servidor de Recarga Online, que implementa um protocolo baseado na norma ISO-8583.

Os equipamentos de autoatendimento se conectarão ao Servidor de Recarga Online através do Serviço Concentrador da rede de distribuição de créditos, da mesma forma que ocorre com os terminais de venda.

## **Requisitos de Software**

As máquinas de autoatendimento deverão ser fornecidas com software, que deverá possuir as características mínimas:

- I. Interação com os dispositivos e periféricos de validação de notas, moedas e Cartões Inteligentes;
- II. Executar as operações de crédito de cartões, de modo *online* e off-line em contingência do mesmo modo que os Pontos de Venda Fixos;
- III. Será apresentado oportunamente pela ARTESP ao vencedor da licitação, os diagramas de estados e interface de telas desejados.

## **8. Equipamentos de Informação ao Usuário**

Vários tipos de equipamentos serão utilizados para fornecer informações aos usuários sobre serviços rodoviários intermunicipais de transporte coletivo de passageiros. Além disso, será possível ao usuário obter informações sobre a viagem que pretende executar e planejar itinerários baseados nas linhas existentes no sistema suburbano e rodoviário. Esses equipamentos deverão ser instalados em todos os 56 polos regionais.

### **8.1. Displays do Sistema de Informação**

Os displays, obrigatórios nos 56 polos regionais, do sistema de informação são aparelhos utilizados para apresentação de imagens tipo vídeo, capacitados para trabalharem como monitores de computador, que fornecem informações textuais aos usuários, oferecendo orientações, informações sobre o tempo, mensagens institucionais e educativas.

### **Especificações técnicas mínimas**

- I. TVs de no mínimo 50 polegadas
- II. Entradas de vídeo VGA e HDMI.
- III. Resolução mínima: 720 x 680 pixels;
- IV. Cores: 16,8 milhões de cores;

- V. Sistemas de cor: NTSC e PAL-M;
- VI. Caixa de Proteção com tela antirreflexo.

## **9. Fornecedores de Itens Pertinentes ao Sistema**

### **9.1. Homologação de Fornecedores e Dispositivos**

No período previsto para a aprovação e homologação do SIBEM pela ARTESP os equipamentos serão submetidos a testes funcionais e ensaios para verificar a aderência aos requisitos da ARTESP, que serão definidos por portaria específica.

Os custos deste processo serão assumidos integralmente pela empresa concessionária.